サイバーセキュリティ検証基盤
の運用に関する
報告書

2021 年 4 月

IPA
独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目 次

図目次（付録 D 及び付録 E を除く）

表 目 次（付 録 D 及 び 付 録 E を 除 く）

用語集・略語集（付録 D 及び付録 E を除く）

本報告書では、以下のとおり用語を定義する。

用語	概要
AP（アクセスポイント）	通信ネットワークの末端でコンピュータなどからの接続要求を受け付け、ネットワークへの通信を仲介する施設や機器のことをいう。
AWS	Amazon Web Services の略。
DoS 攻撃	大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むことをいう。
OSS	Open Source Software の略。
SaaS 型	インターネットを通じてソフトウェアを利用者に提供する方式をいう。
WAF	Web Application Firewall の略。
Wi-Fi Direct	Wi-Fi の通信モードの一つで、固定的なアクセスポイントを介さずに端末同士が直に接続しあって通信するモードをいう。
セキュリティパッチ	ソフトウェアに脆弱性が発見された際に利用者に配布される修正プログラムをいう。
ゼロトラスト	信頼できないことを前提としてセキュリティ対策を講じる考え方をいう。
ファームウェア	コンピュータや電子機器などに内蔵されるソフトウェアの一種で、本体内部の回路や装置などの基本的な制御を司る機能を持ったものをいう。
マルウェア	コンピュータの正常な利用を妨げ、利用者やコンピュータに害を成す不正な動作を行うソフトウェアをいう。

1. 調査概要

1.1 調査背景・目的

経済産業省の産業サイバーセキュリティ研究会 WG3（サイバーセキュリティビジネス化）は、信頼できるセキュリティ製品と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている[1]。これは具体的には、日本で開発されたセキュリティ製品について有効性検証・実環境における試行導入を実施しその結果を発信することで、ユーザーが、日本で開発された製品を選定しやすい環境を構築するものである。

独立行政法人情報処理推進機構（以下「IPA」という。）は、経済産業省の委託を請け、2019 年 9 月にこの事業のあり方を検討する「サイバーセキュリティ検証基盤構築に向けた有識者会議」を設置した。この会議は検証体制や検証方法等の実施案を検討し、その実効性や課題を明らかにするため、少数の製品を題材とした実験的な検証を行った[2]。また、本検証基盤構築の参考とすべく、セキュリティ製品を生み出す社会の仕組みの例について、海外調査を行った。

この活動を通じて得られた知見や明らかになった課題を以下に示す。

(1) 得られた知見

- 日本発のセキュリティ製品には、国内のユーザー企業が直面しているセキュリティ課題の解決に特長・強みを備えた製品が存在する。こうした特長・強みを活かすことで、日本発のセキュリティ製品が海外製品との差別化を図れる可能性がある
- 日本発のセキュリティ製品の特長を専門家が中立・公平に検証し、その結果をユーザー企業に分かりやすく公表することによって、当該製品の市場参入を促進する効果が期待できる

(2) 明らかになった課題

- 検証対象製品は、公平性の観点から広く公募することが望ましい一方、様々な候補製品に対応する一律な審査基準を作ることには困難がある
- 昨年度、実験的に検証作業を実施したところ、製品機能の調査、検証環境構築、製品の挙動分析等にかなりの時間とコストを要した。本基盤の実運用に向けて、一製品あたりの検証に掛かる時間・コストを低減する必要がある
- 本基盤で検証するセキュリティ製品に対し、十分な市場参入の機会を提供するには、それを促進する社会の仕組み（エコシステム）が重要であることが海外調査で再確認された

本事業は 2019 年度に続く二か年目の事業である。2020 年度は、上述の知見・課題を踏ま

[1] 経済産業省「産業サイバーセキュリティ研究会WG３　第４回　事務局説明資料」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/004_03_00.pdf （2020 年 12 月 18 日閲覧）

[2] IPA「セキュリティ製品の有効性検証の試行について」 https://www.ipa.go.jp/security/economics/shikoukekka2019.html （2020 年 12 月 18 日閲覧）

えた上で、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤について、構築を行う。さらに、本基盤を実際に運用して、検証対象候補の製品を公募しその中から対象製品を選定して検証を行う。

さらに、本基盤で検証するセキュリティ製品の市場参入を支援する上で有効な、我が国の状況にあったエコシステムの検討を行う。また加えて、昨年度の成果である「試行導入・導入実績公表の手引き」[3]の改良を行う。

1.2 調査実施概要

業務概要は下記のとおりである。

- サイバーセキュリティ検証基盤の構築
- サイバーセキュリティ検証基盤の運用
- エコシステムの検討
- 19 年度成果「試行導入・導入実績公表の手引き」の改良

本報告書では、このうち、「サイバーセキュリティ検証基盤の運用」に関する内容について記載する。

[3] IPA「試行導入・導入実績公表の手引き」https://www.ipa.go.jp/files/000081564.pdf （2020 年 12 月 18 日閲覧）

2. 重要分野マップの見直し

2.1 重要分野マップの見直し結果

セキュリティ脅威の状況やユーザー企業の状況を加味した上で、IPA により重要分野マップの見直しが行われた。有識者の意見を踏まえ、昨年度の重要分野マップに対して「IT 資産の認証／検証」を加えることとされた。この背景として、ゼロトラストの思想が広まっていることが挙げられる。2020 年 8 月には、米国国立標準技術研究所（NIST）により“Special Publication（SP）800-207: Zero Trust Architecture”の正式版が公開[4]され、ゼロトラスト・アーキテクチャの考えが浸透し始めてきていることが挙げられる。今年度見直された重要分野マップを付録 A に示す。

[4] NIST「SP 800-207: Zero Trust Architecture」https://csrc.nist.gov/publications/detail/sp/800-207/final （2021 年 1 月 18 日閲覧）

3. 製品公募・対象製品選定

3.1 公募対象製品分野の選定結果

見直した重要分野マップを踏まえ、今年度の公募の対象分野を決定した。対象分野として、IPA より以下の 3 分野が提案され、有識者の承認を経て決定された。

① 脅威の可視化：

エンドユーザーやシステム管理者などが晒されているセキュリティ上の脅威を可視化することに資する製品。下記の機能等を想定する。

- マルウェアの感染などによる不審な内部通信の発生を捉え、通知する
- 通信フローを監視し、定常時とは異なる状況を検知した場合に通知する

② 脆弱性の可視化：

OS、ファームウェア、ソフトウェアに含まれる脆弱性を検出し、検出した脆弱性の対策の優先度付けや対策状況を管理することで、脆弱性の可視化に資する製品。下記の機能等を想定する。

- 製品を構成しているオープンソースソフトウェア（以下、「OSS」という）に内在する脆弱性の検出とリスク評価を自動で行い、対策の優先度をつけて表示する
- 発見された脆弱性が内在する OSS を含んだシステム、アプリケーションなどの対策状況を組織単位、ソフトウェア単位などで表示・管理する

③ **IT 資産の認証/検証：**

IT 資産に関する様々な情報（端末情報、OS、アプリ、バージョン、セキュリティパッチ等）に基づいてその信頼性を判断し、認証/検証する製品。下記の機能等を想定している。

- アクセスした端末の真正性（正当性）を判断し、不正な端末の接続を拒否・通知する
- IT 資産におけるアクセスログや操作ログ等を自動で収集し、動作の正当性を検証する

3.2 製品公募実施と選定結果

3.2.1 公募・選定実施スケジュール

構築したサイバーセキュリティ検証基盤の仕組みに基づき、上記の対象分野に該当する製品を検証するために、製品・ベンダーを公募・選定した。公募・選定に係るスケジュールは表 1 に示すとおりである。

表 1　公募・選定の実施スケジュール

プロセス・構成要素	スケジュール	実施事項	実施主体
2. 製品公募 事前周知	2020/11/30 ～2020/12/1	• 有識者による提案及び事務局の調査にて確認した重要分野の製品を開発しているベンダーに対して、公募を開始する旨、事前に周知した。	IPA・ MRI
製品公募の実施・周知	2020/12/2 ～2020/12/10	• IPA のホームページで公募を開始した。なお、質問の受付期間を 2020/12/2～2020/12/4 とした。	IPA・ MRI
3. 製品選定 製品の一次審査	2020/12/10 ～2020/12/11	• 応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づき、必須要件に満足しているかを機械的に審査した。	IPA・ MRI
製品の二次審査	2020/12/11 ～2020/12/15	• 一次審査に合格した製品に対して、製品の差別化ポイントに関する審査を行った。 • 有識者において、各審査項目の合否をそれぞれ審査し、個々人にて採択予定件数の製品を選定していただいた。	有識者
	2020/12/15	• 有識者による審査結果を集約し、選定件数が多い製品上位 2 製品を検証対象製品の候補とした。	IPA・ MRI
	2020/12/16	• 有識者会議において、選定結果を決定した。	有識者・ IPA・ MRI
	2020/12/16 ～2020/12/18	• 選定結果の通知に向けた準備を行った。	IPA・ MRI
製品決定	2020/12/21	• 応募者に対して選定結果を通知した。	IPA

以降ではそれぞれの実施概要について記載する。

3.2.2　製品公募と選定結果

製品公募開始前に、重要分野の製品を開発しているベンダーに対して本事業に関する事前周知を行った。事前周知の対象としては、公開情報調査により今年度の重要分野に該当すると考えられた製品ベンダー、及び、有識者が重要分野に該当する可能性ありとした製品ベンダーとし、計 10 社程度の製品ベンダーに対して事前周知を行った。後に記載するとおり、今年度の公募には計 6 件の応募が寄せられたが、そのうち 4 社は事前周知を行った製品ベンダーであるため、製品ベンダーの応募を促進する観点では事前周知の影響は大きいと考えられる。

サイバーセキュリティ検証基盤の構築における「製品公募の仕組み定式化」において策定した公募要領・仕様書・応募用紙に基づき、製品公募を 2020 年 12 月 2 日から 2020 年 12 月 10 日にかけ製品公募を実施した。その結果、計 6 件の応募が寄せられた。応募がなされた製品に関して、一次審査を行った。一次審査では、応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づいて、応募者の合格／不合格を機械的に審査した。なお、一次審査において、ある応募ベンダーの必須要件への該当に疑念が生じた際に、当該ベンダーに対して電話による必須条件の確認（ヒアリング）を実施した。

一次審査の結果、一つでも必須要件を満たしていないと評価される応募者は不合格とし、一次審査を通過した 4 製品に関して、2020 年 12 月 11 日から 2020 年 12 月 15 日にかけ、有識者による二次審査を実施した。二次審査では、製品の差別化ポイントに関する審査や「日本発」製品であることの判断を行った。二次審査の審査事項は図 1 に示すとおりである。製品の差別化ポイントの審査に当たっては、有識者が審査項目の合否をそれぞれ審査（点数付け）し、評価合計点に基づき、個々人にて最大 2 製品を選定した。

有識者の選定結果を集約した結果、得票数が高い 2 製品は WiSAS（株式会社スプライン・ネットワーク）と GUARDIAX（株式会社グレスアベイル）であった。これらの製品を今年度の有効性検証の対象とすることを有識者会議に諮り、決定した。

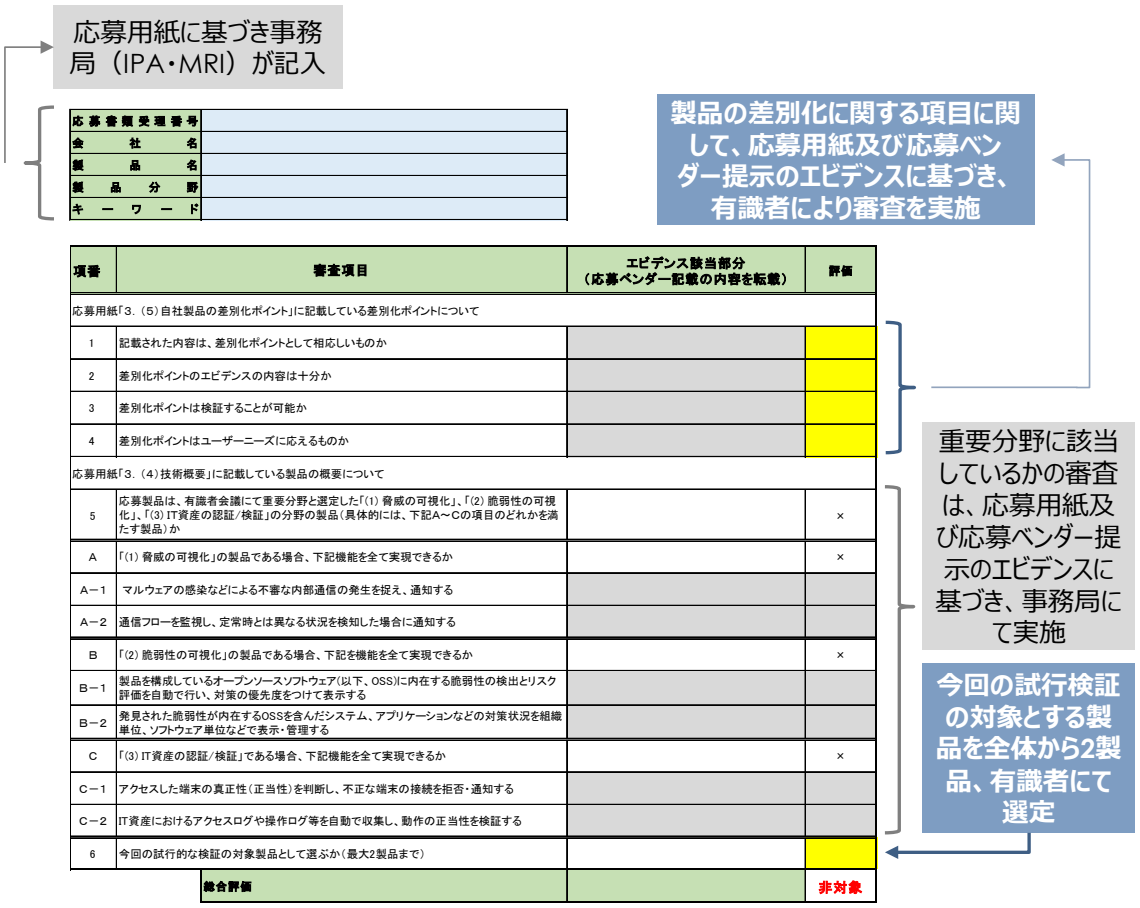
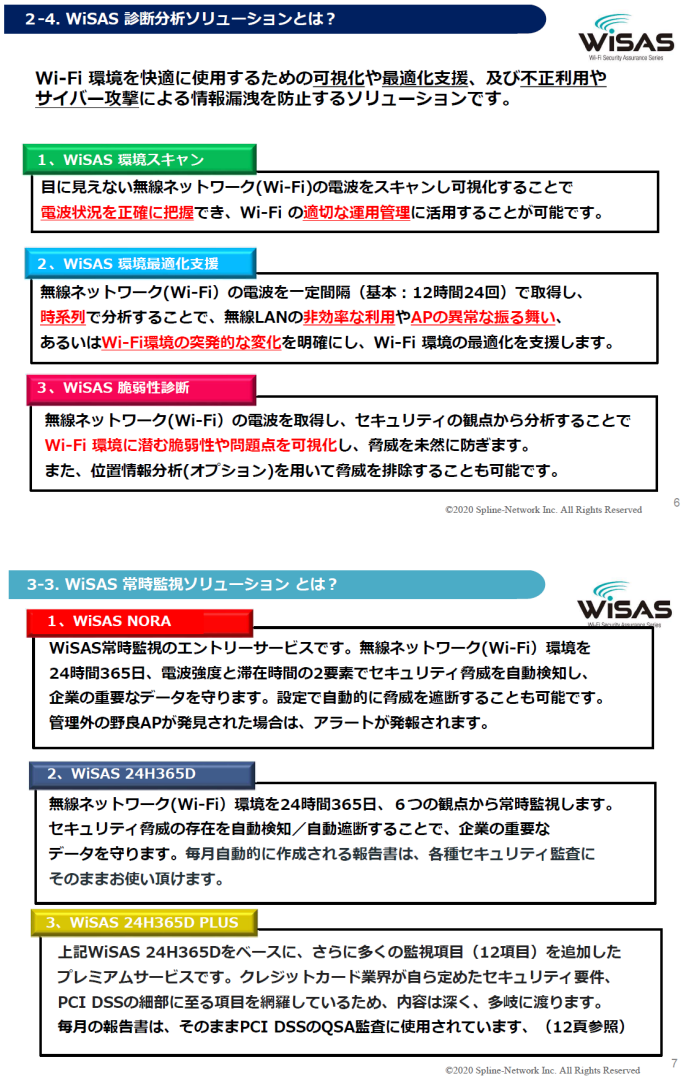


図 1　「製品の二次審査」における審査事項

3.2.3　選定された製品概要

(1) WiSAS（株式会社スプライン・ネットワーク）の概要

株式会社スプライン・ネットワークの製品 WiSAS（Wi-Fi Security Assurance Series）は、Wi-Fi セキュリティに特化した日本発（特許申請中）のソリューションである。ソリューションの概要を図 2 に示す。製品は診断分析ソリューションと常時監視ソリューションの 2 つのカテゴリに分類される。WiSAS センサーを対象エリアに設置し、電源を入れるだけで様々な脅威を検知、及び監視することができ、不正な行為や管理外のアクセスポイントや端末が発見された場合はアラートが発報される。

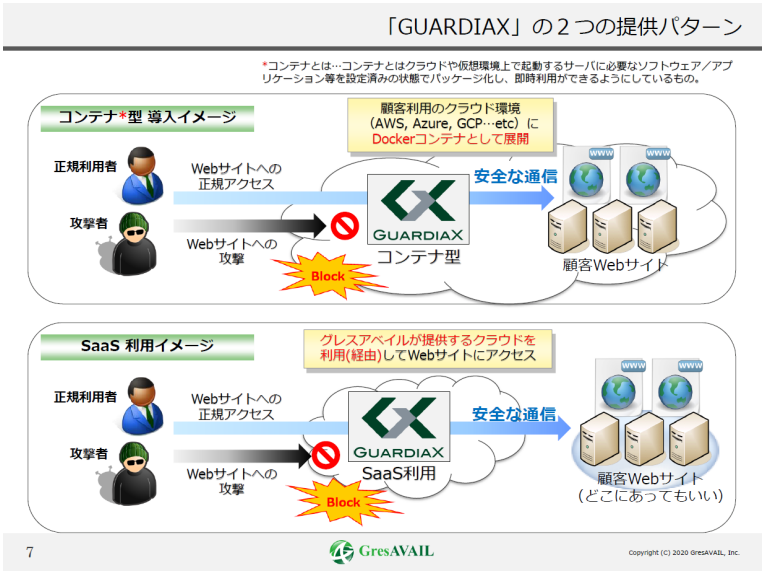


出所）株式会社スプライン・ネットワークの応募用紙・添付資料より

図 2　WiSAS ソリューションの概要

(2) GUARDIAX（株式会社グレスアベイル）の概要

株式会社グレスアベイルの製品 GUARDIAX は SaaS 型／コンテナ型の WAF である。製品の概要を図 3 に示す。Web サイトへの不正アクセスや不正な通信を防止し、その通信の内容を可視化する機能を有するほか、Web サイトへアクセスした端末の詳細を確認する機能を有する。



出所）株式会社グレスアベイルの応募用紙・添付資料

図 3　GUARDIAX ソリューションの概要

4. 検証

4.1 対象製品の機能や差別化ポイントの調査結果

検証実施者（株式会社ラック、以下「ラック」という）は、対象製品ベンダーが製品の強み（以下「差別化ポイント」という）としている事項（下記）をヒアリングし、検証対象の事項として設定した。

4.1.1 WiSAS の差別化ポイントとされている事項

(1) **不正な Wi-Fi AP を検知、遮断できること**
なりすまし Wi-Fi AP（SSID を偽装）、非認可で持ち込まれている Wi-Fi AP、非認可でテザリングに使用されているスマートフォンを検知、通知、遮断し、その位置を二次元平面で特定できる。

(2) **不正な端末の接続を検知、遮断できること**
設置されている正規 Wi-Fi AP に非認可で接続しようとする端末を検知、通知、遮断し、その位置を二次元平面で特定できる。

(3) **Wi-Fi Direct への不正な端末の接続を検知、遮断できること**
複合機やプリンター、プロジェクター、スキャナー等に装備されている Wi-Fi Direct 機能に接続しようとする不正な端末を、検知、通知、遮断、そして、その Wi-Fi Direct 機能が搭載されている機器の位置を二次元平面で特定できる。

(4) **Wi-Fi 環境への DoS 攻撃の有無を確認できること**
Wi-Fi 環境を調査し、DoS 攻撃の有無を確認できる。

4.1.2 GUARDIAX の差別化ポイントとされている事項

(1) **強固な防御ルールであること**
Web アプリケーションの脆弱性を利用した攻撃に対する防御ルールが強固である。

(2) **偽陽性が少ないこと**
偽陽性(正常なアクセスを誤って防御してしまう)が少ないため、短期間(最短 1 日)での導入や利便性の高い運用が可能である。

(3) **攻撃状況が判るダッシュボードが用意されていること**
WAF のダッシュボードにより攻撃（不正アクセス）の状況が判る。

(4) **防御ルールを Web サイト単位でチューニングできること**
Web サイト毎にチューニングした防御ルールを設定できる。

4.2 検証項目・検証方法の策定と策定結果

4.2.1 検証項目・検証方法の策定の進め方

検証項目の策定は表 2 に示すステップにて実施した。また、効率的に検証を実施するために、選定された重要分野に基づき製品決定前に検証項目を仮策定した。重要分野に共通して適用される大分類を「製品機能・性能」、「運用性」、「導入容易性」の 3 つとし、それぞれの大分類に基づき、各重要分野における個別の検証項目を仮策定する。

検証方法の策定においては、仮策定した検証項目に対して、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つのうち、どの方法で検証を行うかを決定した。なお、ベンダーヒアリングに基づく評価は、幅広い項目に適用できる一方で、評価の客観性に欠ける可能性がある。そのため、「検証環境での実検証」及び「データや記録に基づく評価」での検証を基本とし、これら 2 つの手法での検証が難しい項目（ベンダーのノウハウや仕様に係る項目 等）の確認において、例外的に「ベンダーヒアリングに基づく評価」を行うこととした。

仮策定した個別検証項目及び検証方法について、製品の差別化ポイントとされている事項を評価する上で妥当であるかを有識者が審議し、決定した。有識者による検証項目の確認においては、製品ベンダーに確認すべき項目も洗い出した。策定した個別検証項目及び検証方法については次項にて示す。

表 2　検証項目策定ステップ

検証項目の策定ステップ	実施概要	実施主体	実施時期
重要分野の選定	• 有識者会議において検証の対象となる重要分野を選定	有識者	2020/11/6
検証項目 大分類の策定・個別検証項目の仮策定	• 重要分野に共通して適用する検証項目の大分類を策定 • 策定した大分類に基づき、重要分野ごとに、個別検証項目を仮策定	IPA・MRI・ラック	2020/12/4～ 2020/12/16
製品決定			2020/12/18
個別検証項目案の策定	• 選定した製品のベンダーと協議し、製品の差別化ポイントとされている事項を効果的に検証できるよう、仮策定した個別検証項目に加筆修正を行い、個別検証項目の案を策定	IPA・MRI・ラック・応募ベンダー	2020/12/21～ 2021/1/14
個別検証項目案の審議	• 有識者会議において個別検証項目案の妥当性を審議	有識者	2021/1/15～ 2021/1/20
検証項目の確定	• 有識者会議にて、検証項目を確定	IPA・MRI・ラック	2021/1/22

4.2.2　検証項目・検証方法の策定結果

(1) WiSAS の検証項目・検証方法

WiSAS の差別化ポイントとされている事項を検証するため項目を策定した。策定した検証項目のうち、差別化ポイントの検証に特に重要な検証項目を一部抜粋したものを表 3 に示す。全体版は付録 B を参照のこと。

表 3　WiSAS において差別化ポイントとされる事項・検証項目（抜粋版）

検証項目			検証対象の差別化ポイントとされる事項			
区分	No.	検証項目	不正な Wi-Fi AP を検知、遮断できること	不正な端末の接続を検知、遮断できること	Wi-Fi Direct への不正な端末の接続を検知、遮断できること	Wi-Fi 環境への DoS 攻撃の有無を確認できること
認可されていない Wi-Fi AP・端末の検知と遮断	1-1	認可されていない Wi-Fi AP をフロア内に持ち込んだ時、それを検知・遮断し、その AP が設置されている場所を特定できるか	✓			
	1-2	認可されていない端末が、フロア内に設置されている Wi-Fi AP に接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか		✓		
	1-3	フロア内のプリンターに装備されている Wi-Fi Direct 機能が有効にされている時に、認可されていない端末が Wi-Fi Direct に接続された場合、それを検知・遮断できるか			✓	

検証項目			検証対象の差別化ポイントとされる事項			
区分	No.	検証項目	不正な Wi-Fi AP を検知、遮断できること	不正な端末の接続を検知、遮断できること	Wi-Fi Direct への不正な端末の接続を検知、遮断できること	Wi-Fi 環境への DoS 攻撃の有無を確認できること
	1-4	フロア内に設置されている Wi-Fi AP が DoS 攻撃を受けた場合、それを検知できるか、また、レポートされるか				✓
報告書	1-14	不正 Wi-Fi AP の持ち込み、端末の不正接続の対策に有用な情報が記載されているか	✓	✓	✓	✓

各検証項目に対して、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つの方法のうち、どの方法で検証を行うか決定した。決定した検証方法のうち、表 3 で示した検証項目に対する検証方法について一部抜粋したものを表 4 に示す。全体版は付録 B を参照のこと。

表 4　WiSAS の検証項目に対する検証方法（抜粋版）

検証項目			検証方法			
区分	No.	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価	備考
認可されていない Wi-Fi	1-1	認可されていない Wi-Fi AP をフロア内に持ち込んだ時、それを検知・遮断し、その AP が設置さ	✓	✓		実検証の結果提示される報告書も確認した。

検証項目			検証方法			
区分	No.	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価	備考
AP ・端末の検知と遮断		れている場所を特定できるか				
	1-2	認可されていない端末が、フロア内に設置されている Wi-Fi AP に接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか	✓	✓		
	1-3	フロア内のプリンターに装備されている Wi-Fi Direct 機能が有効にされている時に、認可されていない端末が Wi-Fi Direct に接続された場合、それを検知・遮断できるか	✓	✓		
	1-4	フロア内に設置されている Wi-Fi AP が DoS 攻撃を受けた場合、それを検知できるか、また、レポートされるか			✓	DoS 攻撃を実際に実施することが困難なため、ヒアリング、関連資料（過去事例）にて確認した。
報告書	1-14	不正 Wi-Fi AP の持ち込み、端末の不正接続の対策に有用な情報が記載されているか	✓	✓		実検証の結果提示される報告書を確認した。

(2) GUARDIAX の検証項目・検証方法

GUARDIAX の差別化ポイントとされている事項を検証する項目を策定した。策定した検証項目のうち、これら事項の検証に特に重要な検証項目を一部抜粋したものを表 5 に示す。全体版は付録 C を参照のこと。

表 5　GUARDIAX において差別化ポイントとされる事項・検証項目（抜粋版）

検証項目			検証対象の差別化ポイントとされる事項			
区分	No.	検証項目	強固な防御ルールであること	偽陽性が少ないこと	攻撃状況が判るダッシュボードが用意されていること	防御ルールを Web サイト単位でチューニングできること
防御	1-1	他社製 WAF と比較して強固な防御ルールを実現できているか	✓			✓
	1-2	他社製 WAF と比較して偽陽性が少ないか		✓		
報告書	1-4	ダッシュボードにおいて攻撃の有無を確認できるか			✓	
	1-5	ダッシュボードにおいて検知した攻撃の詳細を確認できるか			✓	
	1-6	ダッシュボードにおいて検知した攻撃のレベル分けができるか			✓	

各検証項目に対して、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つの方法のうち、どの方法で検証を行うかを決定した。決定した検証方法のうち、表 5 で示した検証項目に対する検証方法について一部抜粋したものを表 6 に示す。全体版は付録 C を参照のこと。

表 6　GUARDIAX の検証項目に対する検証方法（抜粋版）

検証項目			検証方法			
区分	No.	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価	備考
防御	1-1	他社製 WAF と比較して強固な防御ルールを実現できているか	✓	✓		実検証に加えて、製品ベンダーによる他社製 WAF との比較データも確認した。
	1-2	他社製 WAF と比較して偽陽性が少ないか	✓	✓		
報告書	1-4	ダッシュボードにおいて攻撃の有無を確認できるか	✓			
	1-5	ダッシュボードにおいて検知した攻撃の詳細を確認できるか	✓			
	1-6	ダッシュボードにおいて検知した攻撃のレベル分けができるか	✓			

4.3　検証環境の構築結果

4.3.1　WiSAS の検証環境

検証実施主体であるラック社のオフィスを検証環境として使用した。検証は鉄骨鉄筋コンクリート造（SRC）の 6 階建てビルの 5 階の 1 部に存在している、タテ：約 15m、ヨコ：約 10m、高さ：約 2.7m のフロアにて行った。検証のために本フロアに WiSAS センサーを 3 台設置した。本検証環境における机の位置や間隔等の概略寸法及びセンサー設置位置を図 4 に示す。

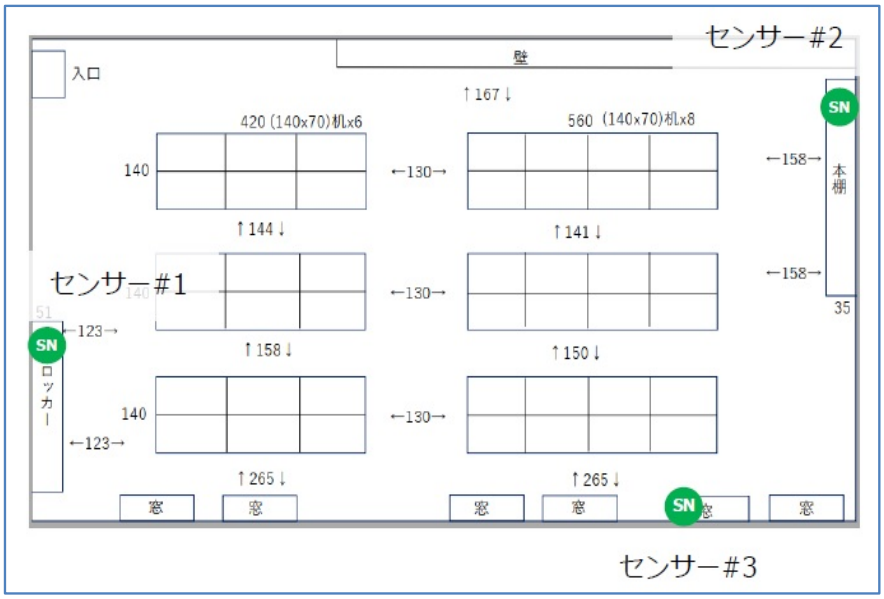


図 4　検証環境概要・WiSAS センサーの設置場所

事前の設定として、2 台の Wi-Fi AP を認可された Wi-Fi AP としてホワイトリストに登録し、1 台のみを検証環境に設置した。また、2 台の端末を認可された端末としてホワイトリストに登録し、検証環境に設置した。その他、ブラックリストに対して Wi-Fi AP 及び端末を登録した。加えて、Wi-Fi Direct 機能を有効にしたプリンター1 台を検証環境に設置した。それぞれの設置場所は図 5 に示すとおりである。

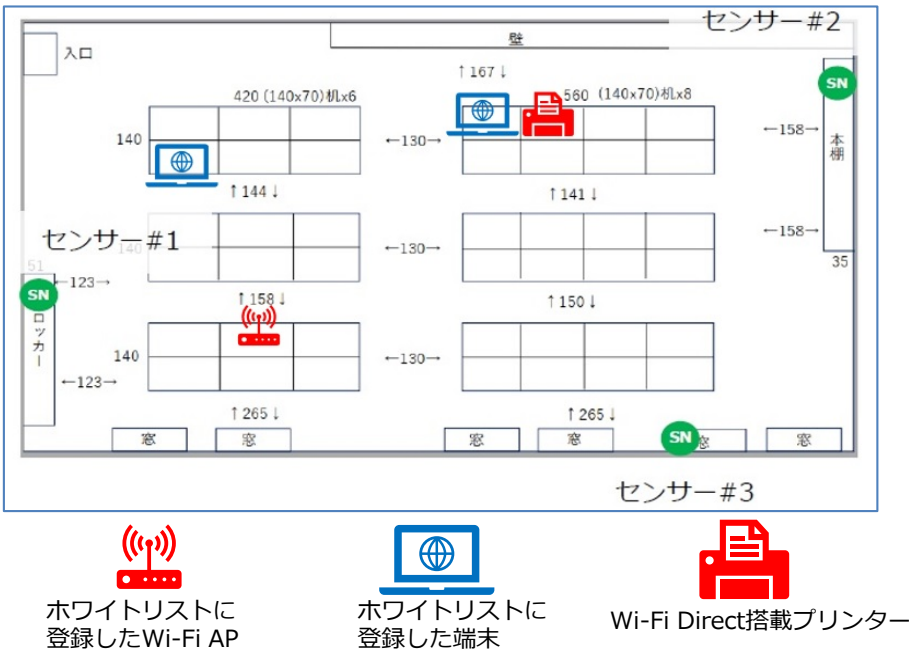


図 5　Wi-Fi AP、端末、Wi-Fi Direct 搭載プリンターの設置場所

この検証環境に対して、認可されていない Wi-Fi AP（テザリング機能を ON にしたスマートフォン）と認可されていない PC を持ち込むことで、それらが検知・遮断されるか等の検証を行った。

なお、WiSAS の利用環境としては多種多様な環境が考えられる。他方で、本有効性検証においては検証できる範囲に限りがあるため、以下の条件に限定して検証を実施した。

- 差別化ポイントとされている検証結果を確認しやすいように、最小限の Wi-Fi AP と端末により検証を実施した。
- センサー群と同じフロアにある Wi-Fi AP／デバイスに対する検知・遮断等の検証を行った。
- 実際のインシデントを調査するのではなく、検証用にインシデントを発生させるシナリオを作成し、そのシナリオに沿って不正な行為を試行し検証した。

4.3.2　GUARDIAX の検証環境

図 6 に示すとおり、AWS にテスト用の Web サイト（hacker.jp）を構築し、GUARDIAX SaaS 版を経由してアクセスする環境を構築した。

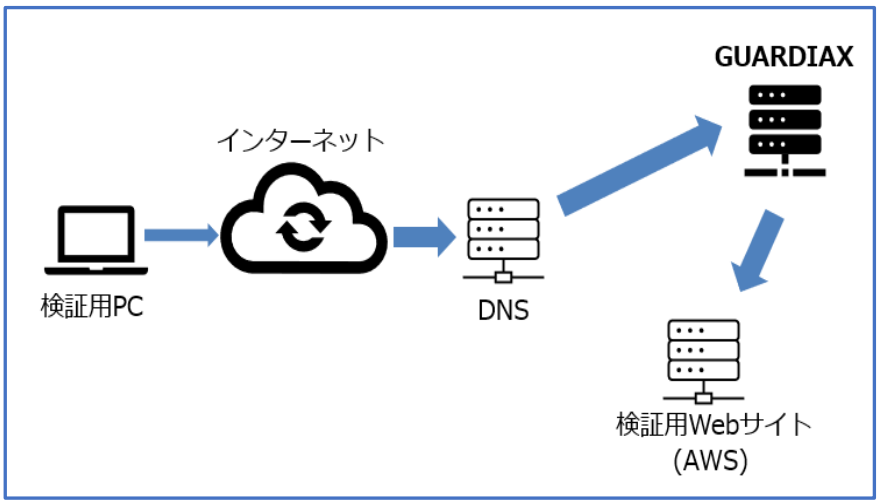


図 6　GUARDIAX の検証環境

GUARDIAX SaaS 版の利用に当たって、まず GUARDIAX 申請書を作成しアカウント情報が提供された後、ダッシュボードにて検証用 Web サイトの FQDN を登録した。その後、ダッシュボードにて防御ルールを設定した。

検証用 Web サイト（AWS）は GUARDIAX からのアクセスのみを IP 制限により許可した。また、防御機能を確認するために、以下に示す通信（HTTP リクエストまたはレスポンス）を一つ以上発生させ、防御機能の有効性や、ダッシュボードにおける表示を検証した。

- スキャニング検出
- クロスサイト・スクリプティング（XSS）
- SQL インジェクション
- OS コマンド・インジェクション
- PHP インジェクション
- 改行コードインジェクション
- LDAP インジェクション
- ローカルファイルインクルード
- リモートファイルインクルード
- Java 攻撃
- Apache Struts2
- ブルートフォースアタック
- EC-CUBE
- クレジットカード情報データ
- SQL エラー
- Java 情報
- PHP 情報
- IIS 情報

- ディレクトリ情報
- CGI 情報

ブルートフォースアタックについては、GUARDIAX のルール設定画面には当該攻撃に関する防御を直接指定する項目が存在しなかったが、登録した Web サイト毎に単一 IP からのリクエスト数を制限する機能が存在したため、これをブルートフォースアタックに対する防御機能として扱う。この機能によって制限されたアクセスは、ダッシュボード上では「アクセス制御」の攻撃種別として表示される。なお、攻撃はプロキシツールである Burp Suite を用いて実施した。

なお、検証する事項のうち「強固な防御ルールであること」及び「偽陽性が少ないこと」については、OWASP が発行している Web アプリケーションセキュリティに関するレポートである OWASP Top 10（2017）に基づいてグレスアベイル社が実施した検証結果と、その結果を参考に実検証した結果に基づき評価を行った。

4.4 検証結果

4.4.1 WiSAS の検証結果

本検証では、ベンダーが対象製品の差別化ポイントとしている 4 つの事項（4.1.1 項）に対して、4.3.1 項に示す検証環境・検証条件の下で検証を行い、その「製品機能・性能」、「運用性」、「導入容易性」について確認した（詳細は付録 D を参照）。

4.4.2 GUARDIAX の検証結果

本検証では、ベンダーが対象製品の差別化ポイントとしている 4 つの事項（4.1.2 項）に対して、4.3.2 項に示す検証環境・検証条件の下で検証を行い、その「製品機能・性能」、「運用性」、「導入容易性」について確認した（詳細は付録 E を参照。）。

5. まとめ・考察

本事業では、昨年度の事業の知見・課題を踏まえた上で、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤について、構築を行った。さらに、構築した本基盤を実際に運用して、検証対象候補の製品を公募しその中から対象製品を選定して検証を行った。

5.1 製品公募・対象製品選定のプロセスについて

まず、製品公募開始前に事前周知を行った。その後、「製品公募の仕組み定式化」において策定した公募要領・仕様書・応募用紙に基づき 10 日間の製品公募を実施したところ、計 6 件の応募が寄せられた。応募がなされた製品に対して製品審査を行い、得票数が高い 2 製品を今年度の対象製品として決定した。

製品公募開始前の事前周知の対象は、公開情報調査により今年度の重要分野に該当すると考えられる製品ベンダー、及び、有識者が重要分野に該当する可能性ありとした製品ベンダーとし、計 10 社程度の製品ベンダーに対して事前周知を行った。今回応募のあった 6 社のベンダーのうち、4 社は事前周知を行った製品ベンダーであり、製品ベンダーの応募を促進する観点で、事前周知の効果は大きいと考えられる。次年度以降の検証基盤の運用においても、製品公募開始前に適切な製品ベンダーに対して事前周知を行うことが効果的である。また、より多くの製品ベンダーによる応募を促進するという観点では、製品公募期間を長期間設定するとともに、それに伴って製品選定・審査の期間も長めに設定することが必要となる。加えて、検証の全体スケジュールにも影響されるが、十分な製品選定期間を設けることができる場合、書面では汲み取れない製品の差別化ポイントを聴取するためのプレゼンテーション機会を設けることも考えられる。なお、プレゼンテーション機会の実施イメージについては、「サイバーセキュリティ検証基盤の構築」に係る報告書にて記載している。

5.2 検証のプロセスについて

対象製品の差別化ポイントとされている事項を確認した後、製品個別の検証項目と検証方法を策定した。今回の重要分野に共通して適用される検証項目の大分類を「製品機能・性能」、「運用性」、「導入容易性」の 3 つとし、この大分類に基づき、各製品に対する個別の検証項目を仮策定した。また、それぞれの検証項目に対して「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つの方法にて検証することを仮策定した。これらの検証項目及び検証方法について、製品の差別化ポイントとされている事項を確認する上で妥当であるかを有識者が審議、決定した。正式に策定された検証項目及び検証方法に基づき、選定された製品に対して検証を行い、その結果を検証結果報告書としてまとめた。

差別化ポイントに関する検証項目の策定に当たっては、当該製品分野に関する専門的な知見や市場環境に関する知見が必要となる。今回選定された 2 製品を例に挙げても、それぞれの製品が解決する課題や市場環境は大きく異なる。WiSAS の場合は、競合製品の存在が限定的であるため、ブルーオーシャン環境における製品とみなすことができるが、GUARDIAX では、WAF の市場がある程度成熟している。それぞれの市場環境が大きく異な

るため、市場環境を踏まえた上で、差別化ポイントに関する検証項目の策定が必要となる。レッドオーシャン環境における製品の場合、競合製品との比較によって差別化ポイントを主張できる場合がある。他方で、本基盤において競合製品を実検証することは困難であるため、レッドオーシャン環境における製品の差別化ポイントの効果的な検証方法については今後も検討が必要である。また、レッドオーシャン環境における製品として、コスト優位性を武器に市場参入を狙っている製品も存在する。「サイバーセキュリティ検証基盤の構築」に係る論点ともいえるが、どのような製品に焦点を当て、有効性検証の対象として選定するかは、市場動向等を踏まえて継続的に検討することが望まれる。

実際の検証に当たっては、それぞれの検証項目に関して、有効な検証シナリオを策定し、それに基づき検証を行うことが重要である。検証シナリオの検討に当たっては、専門的な知見を有する有識者によるレビューを行うことが効果的である。

付録 A：重要分野マップの見直し結果

＜重要分野＞①脅威の可視化、 ②脆弱性の可視化、 ③IT資産管理、 ④脅威インテリジェンスの整理・管理、 ⑤マルウェア感染/発症の重篤度判定、 ⑥教育・トレーニング、 ⑦ハイレベルセキュリティ検証、**⑧IT資産の認証/検証**

組織に対するサイバーセキュリティ脅威(*) ＼ 対策が必要なプロセス		資産管理			リスク管理			防御		監視・検知				対応・復旧				教育・訓練
		IT資産管理	ID/アクセス管理	**IT資産の認証/検証**	脆弱性管理	テスト(ペネトレーションテスト等)	リスクアセスメント	境界防御	データ保護(暗号化)	クラウド/サーバ	ネットワーク	エンドポイント	リアルタイム検知	インシデントレスポンス	分析(フォレンジック)	復旧	サイバー保険	
継続的に存在する脅威	標的型攻撃による機密情報の窃取			○	○		④		○			○		○				○
	内部不正による情報漏えい		○						○	○		○		④	○			⑥
	ビジネスメール詐欺による金銭被害						○					○	⑤	○			○	○
	ランサムウェアによる被害			○								○	○	○			○	○
	予期せぬIT基盤(クラウド、データセンター)の障害に伴う業務停止	③														○	○	○
	不注意による情報漏えい	○		⑧	②				○		①	○						○
	Web上サービスからの個人情報窃取				○		○		○	○				○				
	DDoS攻撃によるサービス停止						○	○		○	○					○		
新たに顕在化した脅威	サプライチェーンの弱点を悪用した攻撃による情報漏えい	○		○	○	⑦	○			○							○	
	IoT機器のBot化などの不正利用、情報漏えい	○		○	○	○	○						○					
	制御系システムへの攻撃による製造ライン停止				○	○	○					○	○					
	シャドーITによる不正アクセス、情報漏えい	○	○	○			○			○			○					
	利用しているオープンソースソフトウェアの脆弱性による不正アクセス、情報漏えい	○			○		○						○	○				

(*)：IPAが2020年1月29日に公開した「情報セキュリティ10大脅威 2020(https://www.ipa.go.jp/security/vuln/10threats2020.html)」の組織編に上げられた脅威に、制御システムへのサイバー攻撃など組織として対策すべき事項を付け加えた

図 7　重要分野マップの見直し結果

付録 B：WiSAS の検証項目・検証方法

表 7　WiSAS の検証項目・検証方法一覧

検証項目				検証対象の差別化ポイントとされる事項				検証方法			
大分類	No.	区分	検証項目	不正なWi-Fi APを検知、遮断できること	不正な端末の接続を検知、遮断できること	Wi-Fi Directへの不正な端末の接続を検知、遮断できること	Wi-Fi環境へのDoS攻撃の有無を確認できること	実検証 検証環境での実検証	データ データや記録に基づく評価	ヒアリング ベンダーヒアリングに基づく評価	備考
製品機能・性能	1-1	認可されていないWi-Fi AP ・端末の検知と遮断	認可されていないWi-Fi APをフロア内に持ち込んだ時、それを検知・遮断し、そのAPが設置されている場所を特定できるか	✓				✓	✓		実検証の結果提示される報告書も確認した。
	1-2		認可されていない端末が、フロア内に設置されているWi-Fi APに接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか		✓			✓	✓		実検証の結果提示される報告書も確認した。
	1-3		フロア内のプリンターに装備されているWi-Fi Direct機能がWi-Fi APとして設定されている時に、認可されていない端末がWi-Fi Directに接続された場合、それを検知・遮断できるか			✓		✓	✓		実検証の結果提示される報告書も確認した。
	1-4		接続を遮断できる端末台数に制限があるか	✓	✓					✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	1-5		フロア内に設置されているWi-Fi APがDoS攻撃を受けた場合、それを検知できるか、また、レポートされるか				✓		✓	✓	DoS攻撃を実際に実施することが困難なため、ヒアリング、関連資料（過去事例）にて確認した。
	1-6	検知タイミング	適切なタイミングでWi-Fi APや接続されている端末を検知しているか	✓	✓	✓	✓			✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	1-7	Wi-Fi AP・端末の管理方法及び設定	認可されたWi-Fi APが登録されたWi-Fi APホワイトリスト、そのWi-Fi APに接続が認可された端末が登録された端末ホワイトリストの作成は容易か	✓	✓			✓			
	1-8		認可しないWi-Fi APが登録されたWi-Fi APブラックリスト、Wi-Fi APに接続を認可しない端末が登録された端末ブラックリストの作成は容易か	✓	✓			✓			
	1-9		一時利用と常時設置Wi-Fi APの識別は容易か	✓				✓	✓		実検証の結果提示される報告書も確認した。
	1-10		一時利用と常時設置Wi-Fi APに接続した端末の識別は容易か		✓			✓	✓		実検証の結果提示される報告書も確認した。
	1-11	通知（アラート）	通知は適切な手段でリアルタイムに実施されるか	✓	✓			✓			
	1-12	報告書	現状のAP／端末リスト及び不正なAP／端末リストの表示仕様は分かり易いか	✓	✓			✓	✓		実検証の結果提示される報告書を確認した。
	1-13		報告書は読み易いか					✓	✓		実検証の結果提示される報告書を確認した。
	1-14		報告書の内容は不正Wi-Fi APの持ち込み、端末の不正接続の対策として有用な情報が記載されているか	✓	✓	✓	✓	✓	✓		実検証の結果提示される報告書を確認した。
運用性	2-1	対障害性	障害時の復旧対応は準備されているか	✓	✓					✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	2-2	習得容易性	当該サービスの活用方法を容易に習得できるか	✓	✓			✓	✓	✓	実検証の結果提示される報告書、ベンダーへのヒアリングも確認した。
	2-3	提供の継続性	今後の事業方針・目標は明確か	✓	✓	✓	✓			✓	ベンダーの方針であるため、ヒアリングによる評価を実施した。
	2-4	拡張性・他製品との連携の可能性	製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか	✓	✓	✓	✓			✓	ベンダーの方針であるため、ヒアリングによる評価を実施した。
導入容易性	3-1	設置の容易性	短時間で導入できるか	✓				✓			
	3-2		作業は1人で可能か	✓				✓			
	3-3		別途必要となる費用は発生するか	✓				✓			
	3-4		用意が必要となる機器はあるか	✓				✓			
	3-5	安全性・機密性	安全性や機密性に問題はないか							✓	仕様書も確認した。

付録 C：GUARDIAX の検証項目・検証方法

表 8　GUARDIAX の検証項目・検証方法一覧

検証項目				検証対象の差別化ポイントとされる事項				検証方法			
大分類	No.	区分	検証項目	強固な防御ルールであること	偽陽性が少ないこと	攻撃状況が判るダッシュボードであること	防御ルールがWebサイト単位でチューニングできること	実検証 検証環境での実検証	データ データや記録に基づく評価	ヒアリング ベンダーヒアリングに基づく評価	備考
製品機能・性能	1-1	防御	他社製WAFと比較して強固な防御ルールを実現できているか	✓			✓	✓	✓		実検証に加えて、製品ベンダーによる他社製WAFとの比較データも確認した。
	1-2		他社製WAFと比較して偽陽性が少ないか		✓			✓	✓		実検証に加えて、製品ベンダーによる他社製WAFとの比較データも確認した。
	1-3		SaaS型とコンテナ型に性能の差異は存在しないか	✓	✓	✓	✓			✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	1-4	ダッシュボード	ダッシュボードにおいて攻撃の有無を確認できるか			✓		✓			
	1-5		ダッシュボードにおいて検知した攻撃の詳細を確認できるか			✓		✓			
	1-6		ダッシュボードにおいて検知した攻撃のレベル分けができるか			✓		✓			
	1-7		ダッシュボードにおいてWebサイトの脆弱性を指摘するか			✓		✓			
運用性	2-1	防御ルールの設定	防御ルールの設定変更の反映のタイミングを設定できるか	✓						✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	2-2	ダッシュボード	攻撃情報は分かり易いか			✓		✓			
	2-3		ログ分析は分かり易いか			✓		✓			
	2-4		防御ルールの更新連絡は存在するか			✓				✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	2-5	対故障性	障害時の復旧対応が準備されているか			✓				✓	ベンダーの設計仕様であるため、ヒアリングによる評価を実施した。
	2-6	習得容易性	当該製品の活用方法を容易に習得できるか			✓		✓			
	2-7	提供の継続性	今後の事業方針・目標は明確か	✓	✓	✓	✓			✓	ベンダーの方針であるため、ヒアリングによる評価を実施した。
	2-8	拡張性・他製品との連携の可能性	製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか	✓	✓	✓	✓			✓	ベンダーの方針であるため、ヒアリングによる評価を実施した。
導入容易性	3-1	導入の容易性	導入するWebサイトやサーバに条件はあるか				✓	✓			
	3-2		導入に至るまでの手続きは簡単か				✓	✓			
	3-3		導入時の設定は簡単か				✓	✓			
	3-4		導入に当たってサービスの停止が必要か				✓	✓			
	3-5		Webアプリケーションに対する変更が必要か				✓	✓			
	3-6		導入までの必要期間は短期間か		✓		✓	✓		✓	実検証に加えて、導入が短期間で可能な理由をヒアリングにより確認した。
	3-7	安全性・機密性	安全性や機密性に問題はないか					✓		✓	実検証に加えて、機密情報の取り扱いについてヒアリングより確認した。

セキュリティ製品の有効性検証の検証結果について

株式会社スプライン・ネットワーク

「Wi-Fi Security Assurance Series (WiSAS)」

目 次

図 目 次

表 目 次

用語集・略語集

本文書では、以下のとおり用語を定義する。

用語	概要
2.4GHz 帯	電波の周波数帯のうち、2.4GHz（2,400MHz）前後の帯域のことをいう。
5GHz 帯	電波の周波数帯のうち、5GHz（5,000MHz）前後の帯域のことをいう。
BPO	Business Process Outsourcing の略で、自社の業務プロセスをまとまった単位で継続的に外部の専門的な企業に委託することをいう。
Beacon Flood 攻撃	DoS 攻撃の手法の一つで、標的に ICMP パケットを短時間の間に大量に送りつける攻撃をいう。
DoS 攻撃	大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むことをいう。
IEEE802.11	IEEE が策定している無線 LAN の標準規格で、「IEEE 802.11a」のように末尾のアルファベットで区別される 30 以上の規格群の全体をいう。
ISMS クラウドセキュリティ認証	クラウドサービスに関する情報セキュリティを適切に管理している組織だと証明するための第三者認証をいう。
LTE	Long Term Evolution の略で、携帯電話・移動体データ通信の技術規格をいう。
MAC アドレス	通信ネットワーク上で各通信主体を一意に識別するために物理的に割り当てられた、48 ビットの識別番号をいう。
PSE マーク	Product Safety Electrical Appliance and Materials の略で、電気用品安全法の基準に適合していることを示すマークをいう。
SIer	企業や行政の情報システムの構築、運用などの業務を一括して請け負う事業者のことをいう。
SLA	サービスを提供する事業者が契約者に対し、どの程度のサービス品質を保証するかを提示したものをいう。
SSID	Service Set Identifier の略で、無線 LAN（Wi-Fi）におけるアクセスポイントの識別名をいう。
Wi-Fi Direct	Wi-Fi の通信モードの一つで、固定的なアクセスポイントを介さずに端末同士が直に接続しあって通信するモードをいう。
iCloud	Apple が提供しているクラウドサービスの名称をいう。
アーカイブ	データを保存するための保管場所や記録形式、保管用にひとまとめに整理されたデータなどをいう。
アップロード	通信回線やネットワークを通じて、別のコンピュータへ能動的にデータを送信することをいう。
クラウド	インターネット等のネットワーク経由で、ユーザーにサービスを提供する形態をいう。

用語	概要
グローバル IP アドレス	インターネットに直に接続された機器に割り当てられる IP アドレスをいう。
テザリング	情報機器が自らをインターネットなどに接続するために内蔵する通信機能を、別の機器をネットワークに接続する中継に用いることをいう。
デジタルフォレンジック	犯罪捜査や法的紛争などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術をいう。
ハッキング	他人のシステムを不正な手段で操作したり、不正に機密情報を入手したりすることをいう。
ハニーポット	ネットワーク上で攻撃者やウイルスなどをおびき寄せるためにわざと攻撃しやすいように見せかけたコンピュータなどのことをいう。
ブラックリスト	通信やアクセスを許可しないアドレスなどのリストをいう。
プロトコル	複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順をいう。
ホワイトリスト	通信やアクセスを許可するアドレスなどのリストをいう。
ルータ	コンピュータネットワークの中継・転送機器の一つで、データの転送経路を選択・制御する機能を持ち、複数の異なるネットワーク間の接続・中継に用いられるものをいう。
技適マーク	電波法令で定めている技術基準に適合している無線機であることを証明するマークをいう。
周波数帯	通信などに用いる周波数の範囲のことをいう。
電波チャンネル	信号の伝送経路として用いられる信号線の束や無線電波の周波数帯をいう。
無線 LAN	電波による無線通信により複数の機器間でデータの送受信を行うネットワークをいう。
無線フレーム	データの送受信単位をいう。

1. はじめに

経済産業省の産業サイバーセキュリティ研究会 WG3（サイバーセキュリティビジネス化）は、信頼できるセキュリティ製品と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている。具体的には、日本で開発されたセキュリティ製品について有効性検証・実環境における試行導入を実施しその結果を発信することで、ユーザーが、日本で開発された製品を選定しやすい環境を構築するものである。

独立行政法人情報処理推進機構（以下「IPA」という。）は、経済産業省の委託を請け、2019 年 9 月にこの事業のあり方を検討する「サイバーセキュリティ検証基盤構築に向けた有識者会議」を設置した。有識者会議の検討において、検証基盤の対象製品を日本発のスタートアップ製品とし、効率的な有効性検証の仕組みとして具体化すること、また今年度は「脅威の可視化」、「脆弱性の可視化」、「IT 資産の認証／検証」に係る製品分野を検証対象とすることを方針とした。

本報告書は、本基盤を試行運用して、検証対象候補の製品を公募しその中から対象製品を選定して有効性検証を行った結果を報告するものである。特に、専門家による客観的な「セキュリティ製品の有効性検証」について今年度は 2 製品を選定して、試行的な検証の題材とし、IPA が事務局となって実際に試行検証を実施した。

以下では、株式会社スプライン・ネットワークの「Wi-Fi Security Assurance Series (WiSAS)」を対象に実施した有効性検証の検証結果について示す。

2. 検証対象製品 WiSAS について

2.1 対象製品を取り巻く環境

企業のオフィス内や工場、商業施設、店舗など多くの場所で、パソコン、スマートフォン、各種端末・機器等を近距離無線通信 Wi-Fi によりネットワークに接続できる環境が広く整ってきている。そのために必要なものが Wi-Fi アクセスポイント（AP）であり、それを設置することで、その近距離にある端末等が無線で通信してネットワークに接続することができる。しかしながら、その Wi-Fi AP と端末等で構成されるネットワークにおいては脅威が存在し、次のような事例が発生している。

- 事例 1 : オフィス内に設置している Wi-Fi AP と同じ SSID、同じパスワードを持つ「なりすまし AP」が不正に設置されており、知らずに接続した端末の通信データが盗聴された。（情報窃取）
- 事例 2 : 社員が個人のスマートフォンのテザリング機能を利用して外部へ通信し、社内のデータを持ち出した。（情報漏洩）
- 事例 3 : 複合機の Wi-Fi Direct 機能が意図せずに有効になっており、そこから社内ネットワークに侵入された。（不正侵入）

2.2 製品概要

WiSAS は、Wi-Fi 環境のセキュリティを担保するために調査・監視するセキュリティソリューションであり、Wi-Fi 環境を快適に使用するための可視化や分析を行い、不正利用やサイバー攻撃による情報漏洩を防止する機能を提供する。WiSAS の大きな特徴として、下記の 3 点が挙げられる。

- 手間いらずの導入：センサーの電源を入れるだけの簡単設置
- 運用が簡単：レポートの毎月自動作成&アーカイブ
- 緊急時にはアラート・遮断：対策まで自動化

WiSAS に関する全てのサービスは既存のシステムを変更することなく、手軽に短期間で、導入することが可能である。また、監視やレポート作成等、復旧を除くほぼ全ての運用は自動化されるため、利用者の手を煩わせないことが特徴として挙げられる。

2.2.1 構成要素

WiSAS は図 2-1 に示すとおり 3 つの要素で構成される。

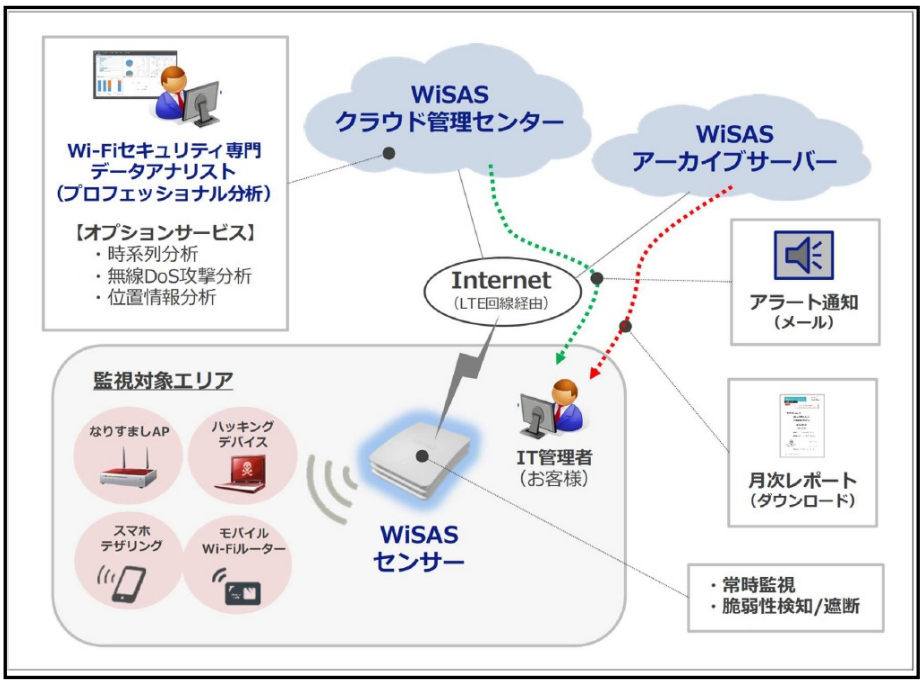


図 2-1　WiSAS の構成要素

WiSAS センサーは Wi-Fi ネットワーク環境を調査及び 24 時間 365 日常時監視し脆弱性（セキュリティリスク）の検知・遮断を自動で実行する機能を搭載した機器であり、監視対象エリアに応じて必要な台数が貸与される。調査・監視できる通信規格は IEEE 802.11 a/b/g/n/ac、周波数帯は 2.4GHz 帯と 5GHz 帯である。

WiSAS センサー1 台で半径 40m～50m 程度（環境要因により変動することに留意）の範囲をカバーする。サービスの利用には、監視対象エリア全体をカバーできる台数を設置する必要がある。同一空間に複数台のセンサーを設置する場合、グループ化して仮想的に 1 台の WiSAS センサーとして動作する。WiSAS センサーは電源を入れるだけで利用でき、既存ネットワーク設備を変更する必要はない。Wi-Fi 環境の監視制御に特化した専用機器のため、無線 AP の機能はない。また、WiSAS センサーは（株）スプライン・ネットワーク社にて全て運用管理（フルマネージド）され、管理サーバーと LTE 回線で通信する。

図 2-2　WiSAS センサーの外観

なお、WiSAS センサーは電源供給に基づき動作するため停電等によって電源供給が無くなった場合は稼働しないが、その場合は利用者に対してアラートメールが送信される。停電等が復旧し、電源供給が復活した場合もメールが送信されるよう設定が可能である。WiSAS センサーは無停電電源装置（UPS）の機能を備えていないが、停電時でも監視を継続した場合は別途 UPS を用意すれば継続的な対策が可能となる。

WiSAS クラウド管理センター（以下「管理センター」という。）には、WiSAS センサー管理サーバー（センサー監視エリアの情報やデータ管理）、各サービスの分析サーバー、死活監視及びインシデントアラートサーバー、報告書作成サーバーなどが含まれている。WiSAS の多種多様なサービスを実現するための機能を備えたクラウドベースの管理センターである。管理センターは（株）スプライン・ネットワーク社にて全て運用管理（フルマネージド）される。フルマネージドによる管理とすることで、WiSAS の有する機能を悪用した外部への攻撃等を防止している。監視対象エリアに設置されたセンサーを一元管理し、センサーによるセキュリティ脅威の検知・遮断に関するログ情報が管理センター内に蓄積される。危険度が高いセキュリティ脅威の検知・遮断が発生した際には、事前に登録された管理者宛にアラート通知のメールを送信する。蓄積されたログ情報から脆弱性の分析を行う。

WiSAS クラウドアーカイブサーバー（以下「アーカイブサーバー」という。）は、常時監視ソリューション導入時に管理センターが作成したレポートを保管するための専用アーカイブサーバーである。クラウドベースで提供され、月次で自動的にレポートが保管される[5]。サービスの提供開始時にアーカイブサーバーのアカウント情報が提供され、ログインすることで保管されているレポートの参照やダウンロードが可能となる。アーカイブサーバーは読み取り権限のみとなり、ファイルの書き込み権限はない。また、レポートは標準で 1 年間保管され、作成から 1 年が経過したレポートはアーカイブサーバーから削除される[6]。

2.2.2 製品によって提供される主なサービス

WiSAS 製品によって主に以下の 6 つのサービスが提供される。

- WiSAS 環境スキャン
- WiSAS 脆弱性診断
- WiSAS 環境最適化支援
- WiSAS NORA（常時監視ソリューション）
- WiSAS 24H365D（常時監視ソリューション）
- WiSAS 24H365D PLUS（常時監視ソリューション）

以降では、今回の有効性検証において利用した「WiSAS 環境スキャン」、「WiSAS 脆弱性診断」、「WiSAS NORA（常時監視ソリューション）」及び「WiSAS 24H365D（常時監視ソリューション）」の 4 つのサービスについて、その概要を記載する。

[5] 保管されるデータは、WiSAS センサーが取得したデータを分析しアナリストのコメントを添えた PDF の報告書が基本となる。ただし、利用者の希望によっては WiSAS センサーが取得したローデータ、及びそれに対してセキュリティ対策に必要な分析をまとめた Excel データの提供も可能となる。

[6] アーカイブ継続希望の利用者には別途延長保管サービスも提供されている。

(1) WiSAS 環境スキャン

Wi-Fi 環境の実態を簡易的に調査するサービスであり、どのような Wi-Fi AP が社内に存在するか把握したい場合や、どの Wi-Fi AP にどの端末が接続しているか把握したい場合に有効である。スキャンの結果は図 2-3 のように一覧化され、報告書として利用者に提示される。報告書では①AP 一覧、②端末一覧（接続状況を含む）のセグメント別に表示される。本サービスの調査では、存在する Wi-Fi AP とその信号強度（dBm）及びそれに接続する端末の MAC アドレス、Wi-Fi AP が使用しているプロトコル、電波チャンネル、認証／暗号化方式を調査項目として活用する。

AP MAC	SSID	SSID分類	認証	暗号化	プロトコル	チャンネル	dBm
XX:XX:XX:4D:B9:B0	SNI-WLAN	隠蔽	WPA2-EAP	AES_CCMP	b/g/n	1	-32
XX:XX:XX:16:C5:B8	iX500-AY1C00XXXX	公開	WPA2-PSK	AES_CCMP	b/g/n	1	-61
XX:XX:XX:28:99:79	Stream39XXX	公開	WPA2-PSK	AES_CCMP	ac	36	-39
XX:XX:XX:C0:90:CE	SNI-Guest	隠蔽	WPA2-PSK	AES_CCMP	a/n	56	-51
XX:XX:XX:40:E4:55	603HWa-40XXXX	公開	WPA2-PSK	AES_CCMP	b/g/n	1	-77
XX:XX:XX:A8:25:51	hm-XX	隠蔽	WPA2-EAP	AES_CCMP	a/n	36	-82
XX:XX:XX:4D:F7:60	SNI-WLAN	隠蔽	WPA2-EAP	AES_CCMP	b/g/n	11	-70
XX:XX:XX:3E:6C:02	XXXX_Bus_Free_Wi-Fi	公開	OPEN	NONE	b/g/n	11	-99
XX:XX:XX:7E:DC:1E	Xperia XXXXXX	公開	WPA2-PSK	AES_CCMP	b/g/n	1	-99
XX:XX:XX:49:AF:41	0000XXXXXX	公開	WPA2-PSK	AES_CCMP	b/g/n	6	-100
XX:XX:XX:49:AF:42	XXXX_Bus_Free_Wi-Fi	公開	OPEN	NONE	b/g/n	6	-100

図 2-3　WiSAS 環境スキャンの実施結果イメージ

(2) WiSAS 脆弱性診断

Wi-Fi 環境の脆弱性を可視化し分析するサービスであり、以下の 6 つの観点を単一契約で診断するサービスである。

- 非認可端末：認可された Wi-Fi AP へ接続した、非認可端末の存在
- 不正行為端末：認可されていない Wi-Fi AP へ接続した、認可端末の存在
- なりすまし AP：SSID が同じ、なりすまし Wi-Fi AP の存在
- MAC 偽装 AP：認可された Wi-Fi AP に MAC アドレスを偽装した Wi-Fi AP の存在
- Wi-Fi Direct AP：Wi-Fi Direct の電波を送出している Wi-Fi AP の存在
- ハッキングデバイス：悪意あるハッキングデバイスの存在

このサービスは、社内の Wi-Fi AP になりすました Wi-Fi AP が設置されていないか確認したい場合、社内の Wi-Fi AP に不正に接続している端末がないか確認したい場合、脆弱性情報が公開されている Wi-Fi AP が存在するか確認したい場合、及び Wi-Fi 環境が DoS 攻撃を受けているか確認したい場合に本サービスが有効である。上記の 6 項目ごとに、診断の結果と項目別の件数、イベントの結果が図 2-4 のように整理され、診断レポートとして利用者に提示される。また、ホワイトリストに登録された Wi-Fi AP を除く Wi-Fi AP の一覧、ホワイトリストに登録された端末を除く端末の一覧、ホワイトリストに登録された Wi-Fi AP の

一覧、及びホワイトリストに登録された端末の一覧の 4 つのデバイス一覧が作成される。

結果
認可APへの非認可(外部/未分類/ゲスト)端末の接続が検知されました。

項目別件数

項目	説明	危険度	検知件数
認可AP外部端末接続	外部端末が内部の認可されたAPに接続している場合	高	1
認可AP未分類端末接続	未分類端末が内部の認可されたAPに接続している場合	高	1

イベント一覧

イベント	内容	危険度	開始時間	終了時間
探知	未分類端末(XX:XX:XX:33:A5:81)が内部の認可されたAP(SSID：SNI-WLAN、MAC：XX:XX:XX:2B:DF:50)に接続	高	2222.09.01 13:49:38	2222.09.01 14:52:32
探知	外部端末(XX:XX:XX:1A:12:53)が内部の認可されたAP(SSID：SNI-WLAN、MAC：XX:XX:XX:2B:DF:50)に接続	高	2222.09.01 14:25:06	2222.09.01 15:01:01

図 2-4　Wi-Fi 脆弱性診断の実施結果イメージ（非認可端末の診断の場合）

(3) WiSAS NORA（常時監視ソリューション）

Wi-Fi 環境を 24 時間 365 日、電波強度と滞在時間の 2 要素でセキュリティ脅威を自動検知するサービスである。特に、認可されていない Wi-Fi AP が存在するか監視するとともに、認可されていない Wi-Fi AP に接続した端末及びその接続時間を監視する。大きく常時設置と一時利用に分けられ、信号強度や滞在時間に関してそれぞれ閾値を設けられているが、利用者の希望によって変更できる。認可されていない Wi-Fi AP やそれに対して接続した端末が検出された場合、図 2-5 のようにその閾値によって危険度を判断し、接続を遮断し、利用者に対して通知する。また、月次のレポートを自動的に生成し、利用者に対して提示する。

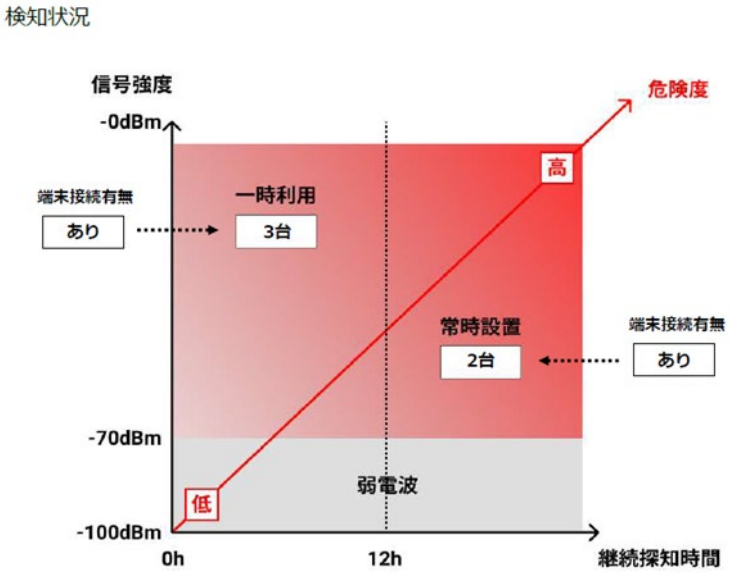


図 2-5　WiSAS NORA サービスにおける端末検知状況のイメージ

(4) WiSAS 24H365D（常時監視ソリューション）

Wi-Fi 環境を 24 時間 365 日常時監視するサービスであり、「(2) WiSAS 脆弱性診断」と同様に以下の 6 つの観点を監視する。

- 非認可端末：認可された Wi-Fi AP へ接続した、非認可端末の存在
- 不正行為端末：認可されていない Wi-Fi AP へ接続した、認可端末の存在
- なりすまし AP：SSID が同じ、なりすまし Wi-Fi AP の存在
- MAC 偽装 AP：認可された Wi-Fi AP に MAC アドレスを偽装した Wi-Fi AP の存在
- Wi-Fi Direct AP：Wi-Fi Direct の電波を送出している Wi-Fi AP の存在
- ハッキングデバイス：悪意あるハッキングデバイスの存在

これらの中でも危険度の高いイベントを検知した場合、その接続を遮断し、利用者に対して通知する。また、月次のレポートを自動的に生成し、利用者に対して提示する。オプション機能として、検知した Wi-Fi AP、接続した端末、Wi-Fi Direct 搭載機器等の位置情報をフロア図面にマッピングしてレポートする。社内の認可されていない Wi-Fi AP を検知・遮断したい場合、社内の正規 Wi-Fi AP に接続された認可されていない端末を検知・遮断したい場合、Wi-Fi Direct 機能が意図せずに有効になっていて認可されていない端末が接続した場合に検知・遮断したい場合等に有効である。

2.3 製品の導入事例

2.3.1 大手 BPO 企業での導入事例

ある BPO（Business Process Outsourcing）企業の執務室で WiSAS を導入したところ、管理外のポータブル Wi-Fi ルータの持ち込みがなされていることが検知された。その後の調査により、顧客データを含む業務上の機密データを iCloud 上にアップロードしていたことが判明した。

2.3.2 大手デジタル放送配信会社での導入事例

ある大手デジタル放送配信会社に WiSAS の脆弱性診断サービス（無線 DoS 攻撃分析及び位置情報分析を含む）と環境最適化支援サービスを導入したところ、従業員が私物スマホのテザリングで会社貸与の PC を利用していることを複数検知した。不正使用機器の位置情報については、位置情報分析サービスによって特定された。また、意図せず有効化された Wi-Fi Direct 機器（プリンター、スキャナー等）を複数検知した。無線 DoS 攻撃分析では、無認可の Wi-Fi AP による無線 DoS 攻撃（Beacon Flood 攻撃）が実施されたことが検知された。後の調査により接続不良が原因であることが特定された。

2.3.3 製造会社での導入事例

ある製造会社に WiSAS 脆弱性診断サービスを導入したところ、内部ネットワークに接続された小型無線 Wi-Fi AP を発見した。後の調査の結果、従業員に賄賂を渡して設置されたことが判明した。産業スパイが介在したと考えられる。

2.3.4　大手 SIer での導入事例

ある大手 SIer に WiSAS 脆弱性診断サービスを導入したところ、従業員が私物スマホのテザリングで会社貸与の PC を利用していることを複数検知した。また、意図せず有効化された Wi-Fi Direct 機器（プリンター、スキャナー等）を複数検知した。加えて、社内の無線 Wi-Fi AP になりすましたハニーポット Wi-Fi AP の存在を検知した。

3. 検証する差別化ポイント・検証項目

3.1 検証対象の差別化ポイントとされる事項

WiSAS の差別化ポイントとされる事項のうち、本検証では以下の 4 つの事項に対して検証を実施した。

(1) **不正な Wi-Fi AP を検知、遮断できること**
なりすまし Wi-Fi AP（SSID を偽装）、非認可で持ち込まれている Wi-Fi AP、非認可でテザリングに使用されているスマートフォンを検知、通知、遮断し、その位置を二次元平面で特定できる。

(2) **不正な端末の接続を検知、遮断できること**
設置されている正規 Wi-Fi AP に非認可で接続しようとする端末を検知、通知、遮断し、その位置を二次元平面で特定できる。

(3) **Wi-Fi Direct への不正な端末の接続を検知、遮断できること**
複合機やプリンター、プロジェクター、スキャナー等に装備されている Wi-Fi Direct 機能に接続しようとする不正な端末を、検知、通知、遮断、そして、その Wi-Fi Direct 機能が搭載されている機器の位置を二次元平面で特定できる。

(4) **Wi-Fi 環境への DoS 攻撃の有無を確認できること**
Wi-Fi 環境を調査し、DoS 攻撃の有無を確認できる。

3.2 検証項目

本検証基盤では、重要分野に共通して適用される検証項目の大分類を策定し、それぞれの大分類の下に選定された各製品の個別検証項目を策定する形式とした。今年度の有効性検証においては、重要分野に共通して適用される大分類を「製品機能・性能」、「運用性」、「導入容易性」の 3 つとした。

3.2.1 製品機能・性能に関する検証項目

WiSAS の差別化ポイントとされる事項を踏まえ、製品機能・性能に関して、表 3-1 に示す検証項目について検証した。

表 3-1 製品機能・性能に関する検証項目

No.	区分	検証項目
1-1	認可されていない Wi-Fi AP・端末の検知と遮断	認可されていない Wi-Fi AP をフロア内に持ち込んだ時、それを検知・遮断し、その AP が設置されている場所を特定できるか
1-2		認可されていない端末が、フロア内に設置されている正規 Wi-Fi AP に接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか
1-3		フロア内のプリンターに装備されている Wi-Fi Direct 機能が有効にされている時に、認可されていない端末が Wi-Fi Direct に接続された場合、それを検知・遮断できるか
1-4		接続を遮断できる端末台数に制限があるか

No.	区分	検証項目
1-5		フロア内に設置されている Wi-Fi AP が DoS 攻撃を受けた場合、それを検知できるか、また、レポートされるか
1-6	検知タイミング	適切なタイミングで Wi-Fi AP や接続されている端末を検知しているか
1-7	Wi-Fi AP・端末の管理方法及び設定	認可された Wi-Fi AP が登録された Wi-Fi AP ホワイトリスト、その Wi-Fi AP に接続が認可された端末が登録された端末ホワイトリストの作成は容易か
1-8		認可しない Wi-Fi AP が登録された Wi-Fi AP ブラックリスト、認可された Wi-Fi AP に接続を認可しない端末が登録された端末ブラックリストの作成は容易か
1-9		一時利用と常時設置 Wi-Fi AP の識別は容易か
1-10		一時利用と常時設置 Wi-Fi AP に接続した端末の識別は容易か
1-11	通知（アラート）	通知は適切な手段でリアルタイムに実施されるか
1-12	報告書	現状の AP／端末リスト及び不正な AP／端末リストの表示仕様は分かり易いか
1-13		報告書は読み易いか
1-14		報告書の内容は不正 Wi-Fi AP の持ち込み、端末の不正接続の対策として有用な情報が記載されているか

3.2.2 運用性に関する検証項目

WiSAS の差別化ポイントとされる事項を踏まえ、運用性に関して、表 3-2 に示す検証項目について検証した。

表 3-2 運用性に関する検証項目

No.	区分	検証項目
2-1	対障害性	障害時の復旧対応は準備されているか
2-2	習得容易性	当該サービスの活用方法を容易に習得できるか
2-3	提供の継続性	今後の事業方針・目標は明確か
2-4	拡張性・他製品との連携の可能性	製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか

3.2.3 導入容易性に関する検証項目

WiSAS の差別化ポイントとされる事項を踏まえ、導入容易性に関して、表 3-3 に示す検証項目について検証した。

表 3-3　導入容易性に関する検証項目

No.	区分	検証項目
3-1	設置の容易性	短時間で導入できるか
3-2		作業は 1 人で可能か
3-3		別途必要となる費用は発生するか
3-4		用意が必要となる機器はあるか
3-5	安全性・機密性	安全性や機密性に問題はないか

4. 検証環境・検証条件

4.1 検証環境の構築

検証は鉄骨鉄筋コンクリート造（SRC）の 6 階建てビルの 5 階の 1 部に存在している、タテ：約 15m、ヨコ：約 10m、高さ：約 2.7m のフロアにて行った。検証のために本フロアに WiSAS センサーを 3 台設置した。本検証環境における机の位置や間隔等の概略寸法及びセンサー設置位置を図 4-1 に示す。

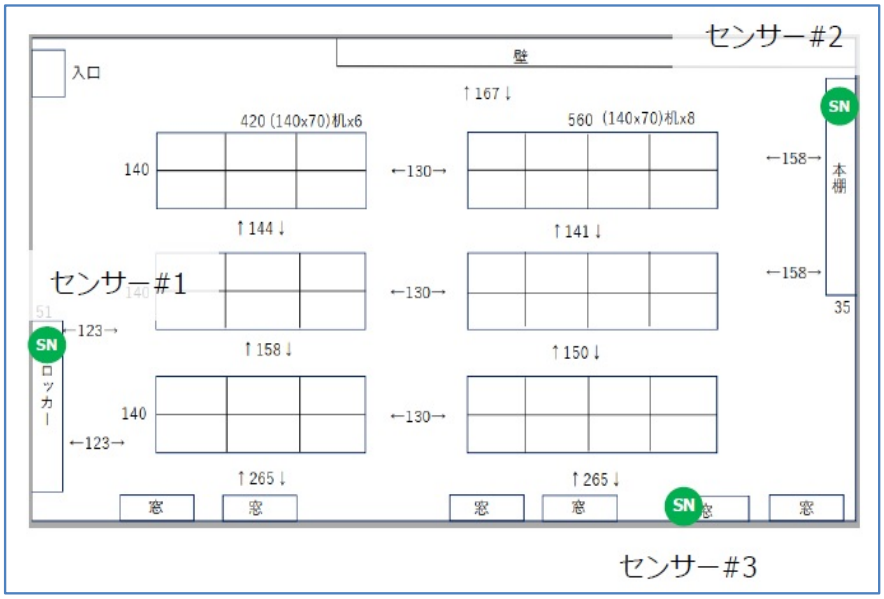


図 4-1　検証環境概要・WiSAS センサーの設置場所

事前の設定として、2 台の Wi-Fi AP を認可された Wi-Fi AP としてホワイトリストに登録し、1 台のみを検証環境に設置した。また、2 台の端末を認可された端末としてホワイトリストに登録し、検証環境に設置した。その他、ブラックリストに対して Wi-Fi AP 及び端末を登録した。加えて、Wi-Fi Direct 機能を有効にしたプリンター1 台を検証環境に設置した。それぞれの設置場所は図 4-2 に示すとおりである。

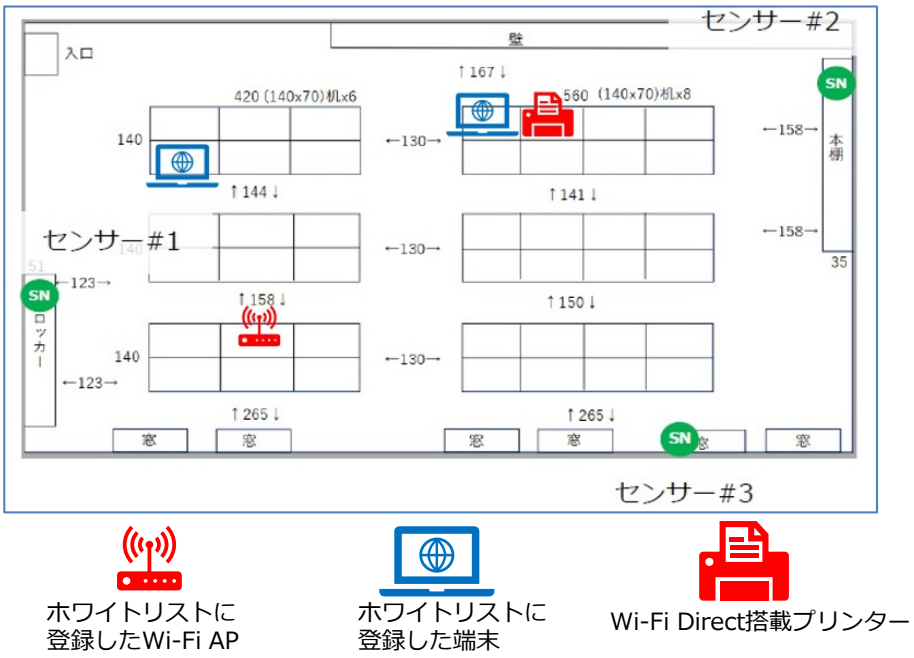


図 4-2　Wi-Fi AP、端末、Wi-Fi Direct 搭載プリンターの設置場所

この検証環境に対して、認可されていない Wi-Fi AP（テザリング機能を ON にしたスマートフォン）と認可されていない PC を持ち込むことで、それらが検知・遮断されるか等の検証を行った。

4.2　検証条件

WiSAS の利用環境としては多種多様な環境が考えられる。他方で、本有効性検証においては検証できる範囲に限りがあるため、以下の条件に限定して検証を実施した。

- 差別化ポイントとされる項目の検証結果を確認し易いように、最小限の Wi-Fi AP と端末により検証を実施した。
- センサー群と同じフロアにある Wi-Fi AP／デバイスに対する検知・遮断等の検証を行った。
- 実際のインシデントを調査するのではなく、検証用にインシデントを発生させるシナリオを作成し、そのシナリオに沿って不正な行為を試行し検証した。

5. 検証結果

5.1 製品機能・性能に関する検証結果

5.1.1 検証項目 1-1 の検証結果

(1) 検証項目の内容

認可されていない Wi-Fi AP をフロア内に持ち込んだ時、それを検知・遮断し、その AP が設置されている場所を特定できるか

(2) 検証結果

認可されている Wi-Fi AP と同じ SSID になりすました AP が検知・遮断できた。また、その AP が設置されている場所を特定できた。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS 24H365D（常時監視サービス）を 3 日間の期間で導入し、ホワイトリストに登録した Wi-Fi AP と同じ SSID の Wi-Fi AP を持ち込むことで検証を行った。実検証によって、ホワイトリストに登録された端末が接続できないことを確認した。また、図 5-1 のとおり接続を遮断した旨のメールがリアルタイムで届いた。

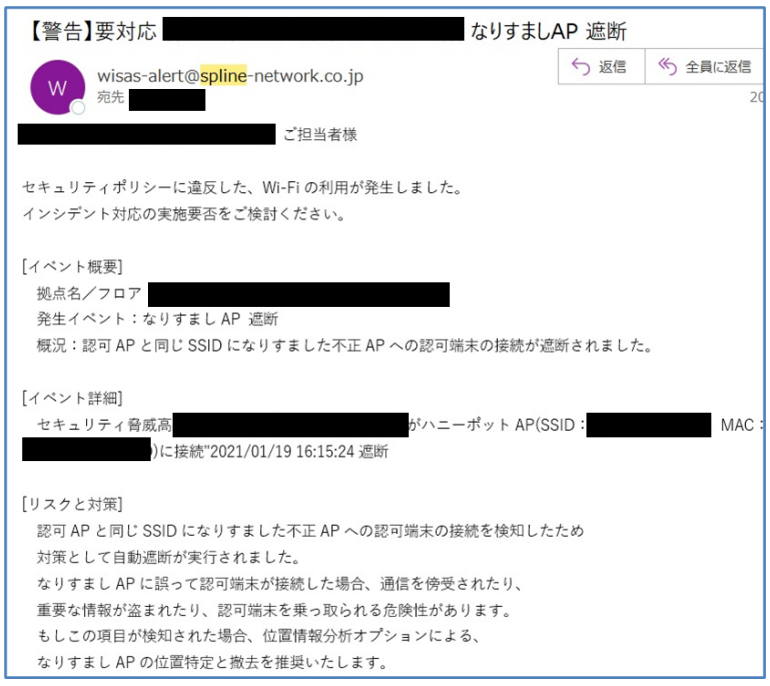


図 5-1 なりすまし AP の遮断を示すメール通知

図 5-2 が WiSAS 24H365D（常時監視サービス）の月次で提示される診断レポートの報告書結果であり、診断レポートからも認可されている Wi-Fi AP と同じ SSID になりすました

AP を検知・遮断したことを確認した。なお、報告書ではなりすまし AP に関するイベントの一覧（発生した内容、危険度、開始時期、終了時期）も提示される。

WiSAS

Spline Network

Confidential

C-3：なりすましAP

この項目のポイント

この項目では、認可APと同じSSIDになりすました不正なAPの存在を検知します。
なりすましAPに誤って認可端末が接続した場合、通信を傍受されたり、重要な情報が盗まれたり、認可端末を乗っ取られる危険性があります。
もしこの項目が検知された場合、位置情報分析オプションによる、なりすましAPの位置特定と撤去を推奨いたします。
さらに、対策として「WiSAS常時監視ソリューション」による、なりすましAPの常時監視および自動接続遮断機能の設定を推奨いたします。

結果

認可APと同じSSIDになりすましたAPが検知されました。

項目別件数

項目	説明	危険度	検知件数
なりすましAP探知	非認可APが社内の認可APと同じSSIDを使用している場合	中	2
なりすましAP認可端末接続	認可端末がなりすましAPに接続している場合	高	0

図 5-2　なりすまし AP の検知・遮断結果

特定したなりすまし AP の位置情報について、報告書により図 5-3 のとおり報告された。実際のなりすまし AP（テザリング機能を有効にしたスマートフォン）の位置の誤差は約 0.5m であり、ほぼ正確に位置が特定できたと考えられる。

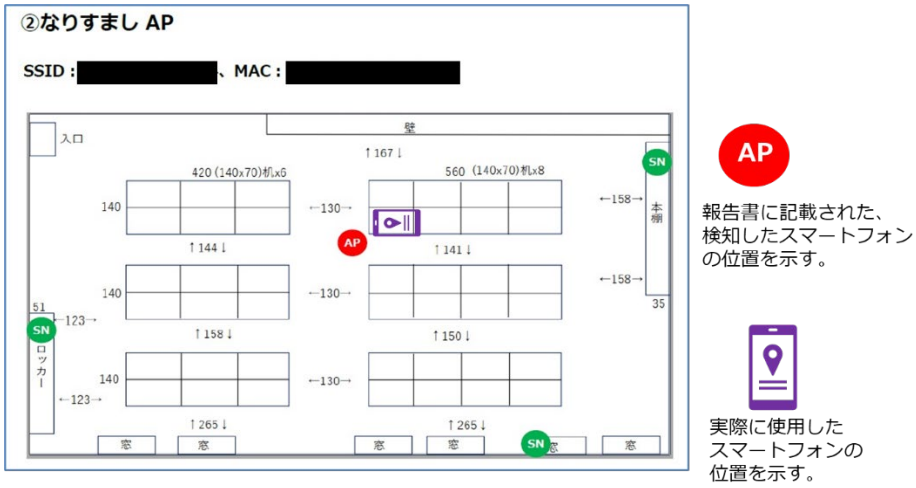


図 5-3　なりすまし AP の位置特定結果

WiSAS は MAC アドレスに基づき遮断を実行する。サービス申込みの段階で遮断の設定を有効化している場合、正規な Wi-Fi AP と MAC アドレスをなりすました Wi-Fi AP に関わらず遮断が実行される。それにより、正規の Wi-Fi AP と正規端末の接続も遮断されるため、設置場所において、MAC アドレスをなりすました Wi-Fi AP の排除と、正規な Wi-Fi AP・正

規端末の復旧が必要となる。したがって、Wi-Fi 環境を安全かつ継続的に運用するためには、WiSAS センサーを設置するだけでなく、図 5-1 のような通知が届いた際に、可能な限り素早く対応できる体制を設置者にて設けることが必要である。

5.1.2　検証項目 1-2 の検証結果

(1) 検証項目の内容

認可されていない端末が、フロア内に設置されている正規 Wi-Fi AP に接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか

(2) 検証結果

認可されている Wi-Fi AP に対して、認可されていない端末が接続した場合に、その端末を検知できた。また、その端末が設置されている場所を特定できた。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS 24H365D（常時監視サービス）を 3 日間の期間で導入し、ホワイトリストに登録した Wi-Fi AP に対して、ホワイトリストに登録していない PC を接続することで検証を行った。実検証によって、ホワイトリストに登録されていない PC が、ホワイトリストに登録された Wi-Fi AP に接続できないことを確認した。また、図 5-4 のとおり接続を遮断した旨のメールがリアルタイムで届いた。

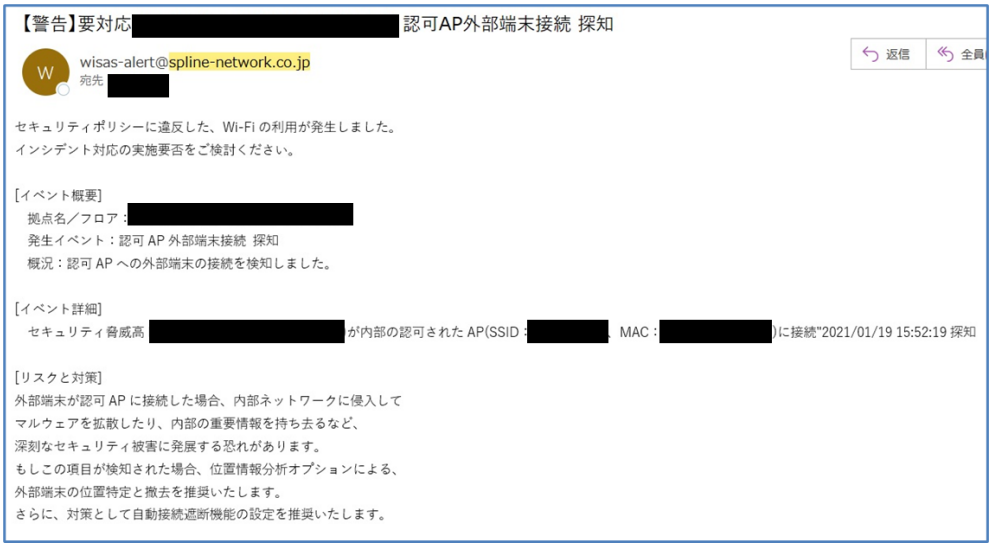


図 5-4　認可されていない端末の遮断を示すメール通知

図 5-5 が WiSAS 24H365D（常時監視サービス）の月次で提示される診断レポートの報告書結果であり、診断レポートからも認可されている Wi-Fi AP に対して、認可されていない端末が接続した場合に、その端末を検知・遮断したことを確認した。なお、報告書では認可されていない端末に関するイベントの一覧（発生した内容、危険度、開始時期、終了時期）

も提示される。

WiSAS Wi-Fi Security Assurance Series

Spline Network

Confidential

C-1：非認可端末

この項目のポイント
この項目では、認可APへの非認可端末(外部/未分類※1)の接続を検知します。 非認可端末が認可APに接続した場合、内部ネットワークに侵入してマルウェアを拡散したり、内部の重要情報を持ち去るなど、深刻なセキュリティ被害に発展する恐れがあります。 もしこの項目が検知された場合、位置情報分析オプションによる、非認可端末の位置特定と撤去を推奨いたします。 さらに、対策として「WiSAS常時監視ソリューション」による、非認可端末の常時監視および自動接続遮断機能の設定を推奨いたします。 ※1…未分類とは探知されてから10分以内に探知されなくなったAPおよび端末です。ドライブレコーダーやバスのWi-Fiなど、短時間の利用や通りすがりの電波が未分類となります。（以後同様）

結果
認可APへの非認可(外部/未分類/ゲスト)端末の接続が検知されました。

項目別件数

項目	説明	危険度	検知件数
認可AP外部端末接続	外部端末が内部の認可されたAPに接続している場合	高	3
認可AP未分類端末接続	未分類端末が内部の認可されたAPに接続している場合	高	10

図 5-5　認可されていない端末の検知・遮断結果

特定した認可されていない端末の位置情報について、報告書により図 5-6 のとおり報告された。実際の端末との位置の誤差は約 2m、Wi-Fi AP との位置の誤差は約 3m であり、捜索により端末を特定することが可能であると考えられる。

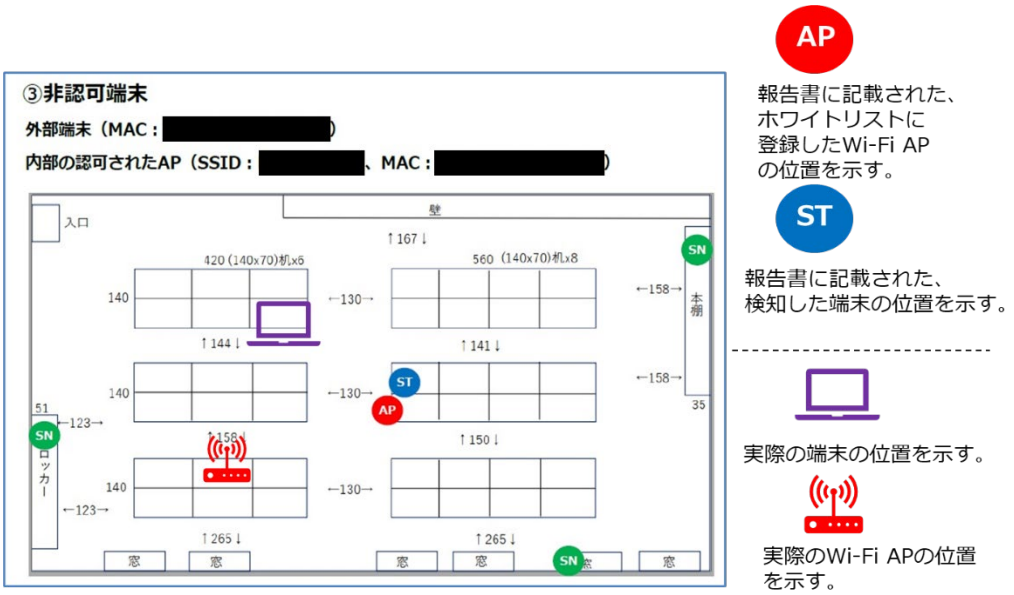


図 5-6　認可されていない端末の位置特定結果

5.1.3　検証項目 1-3 の検証結果

(1) 検証項目の内容

フロア内のプリンターに装備されている Wi-Fi Direct 機能が有効にされている時に、認可されていない端末が Wi-Fi Direct に接続された場合、それを検知・遮断できるか

(2) 検証結果

Wi-Fi Direct 機能が有効にされてプリンターに対して、認可されていない端末が Wi-Fi Direct に接続された場合、それを検知・遮断することができた。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS 24H365D（常時監視サービス）を 3 日間の期間で導入し、Wi-Fi Direct 機能を有効にしたプリンターに対して、認可されていない PC を接続した。実検証によって、認可されていない PC が Wi-Fi Direct 機能に接続できないことを確認した。また、図 5-7 のとおり接続を遮断した旨のメールがリアルタイムで届いた。

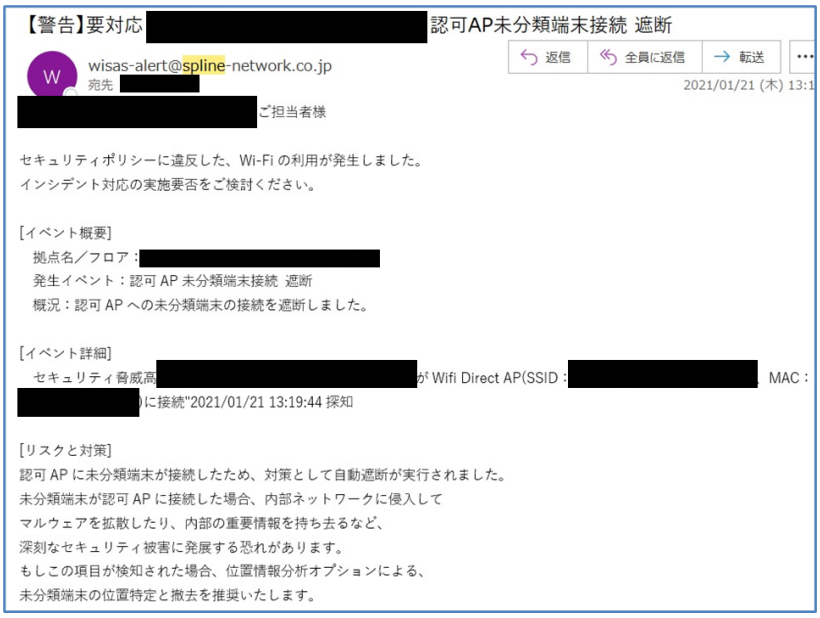


図 5-7　Wi-Fi Direct 機器へ接続した認可されていない端末の遮断を示すメール通知

図 5-8 が WiSAS 24H365D（常時監視サービス）の月次で提示される診断レポートの報告書結果であり、Wi-Fi Direct 機能を有効にしたプリンターに対して認可されていない端末が接続した場合に、その端末を検知できることを確認した。なお、報告書では Wi-Fi Direct AP 及び端末が Wi-Fi Direct AP に接続した場合のイベントの一覧（発生した内容、危険度、開始時期、終了時期）も提示される。

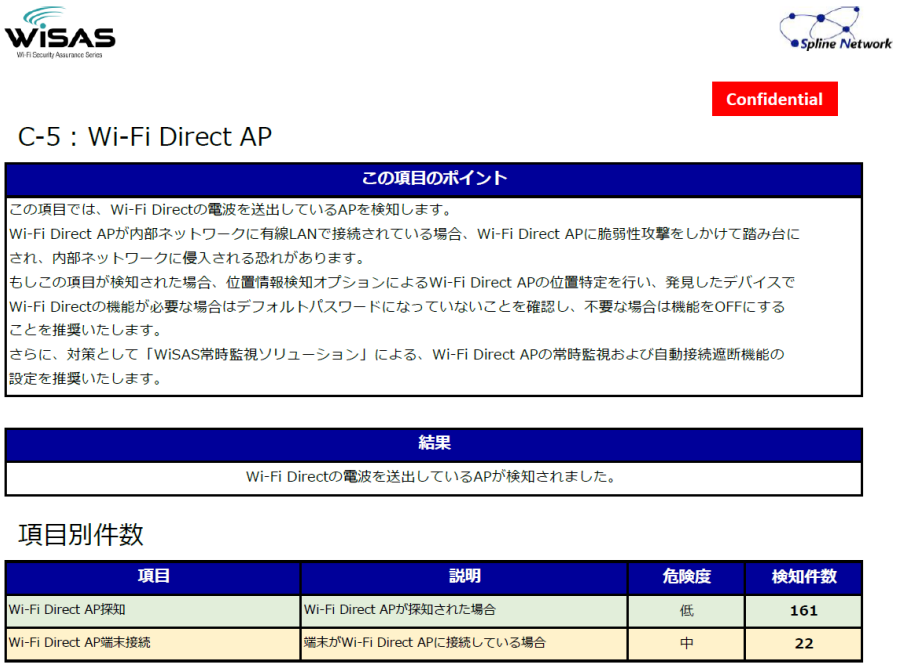


図 5-8　Wi-Fi Direct へ接続した認可されていない端末の検知・遮断結果

特定した認可されていない端末の位置情報について、報告書により図 5-9 のとおり報告された。実際の Wi-Fi Direct 機能を有効にしたプリンターとの位置の誤差は約 1m であり、

ほぼ正確に位置を特定できていると考えられる。

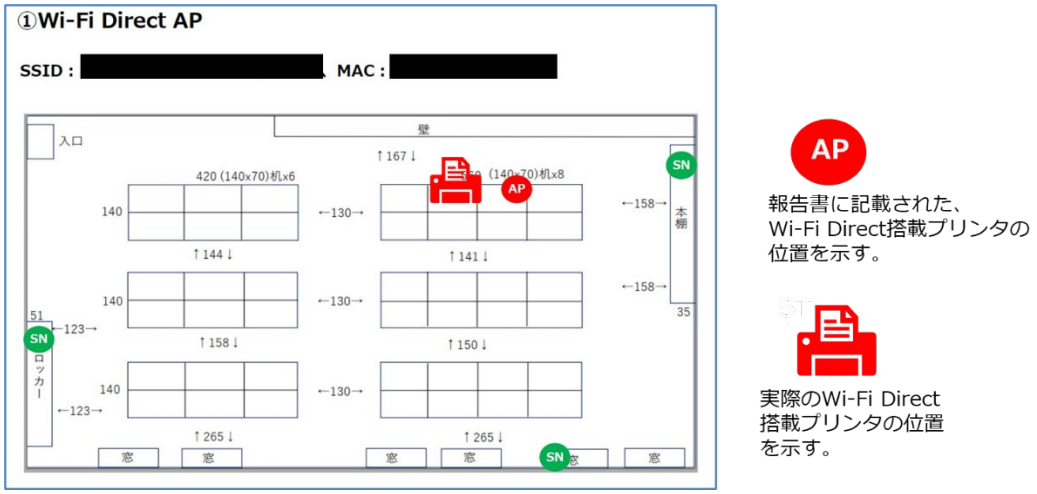


図 5-9　Wi-Fi Direct へ接続した認可されていない端末の位置特定結果

5.1.4　検証項目 1-4 の検証結果

(1) 検証項目の内容

接続を遮断できる端末台数に制限があるか

(2) 検証結果

接続を遮断できる端末台数に制限がないことを確認した。

(3) 検証内容の詳細

製品ベンダーに対するヒアリングにより確認した。ヒアリングにより、接続を遮断できる端末台数に制限がないことを確認した。

5.1.5　検証項目 1-5 の検証結果

(1) 検証項目の内容

フロア内に設置されている Wi-Fi AP が DoS 攻撃を受けた場合、それを検知できるか、また、レポートされるか

(2) 検証結果

過去の事例より、Wi-Fi AP が DoS 攻撃を受けた場合に検知し、レポートできることを確認した。

(3) 検証内容の詳細

製品ベンダーに対するヒアリング及び関連資料の確認により評価した。WiSAS における無線 DoS 攻撃の分析はオプション機能であり、WiSAS センサーが周囲の無線フレームの送信状況をモニタリングし、「壊れた無線フレームの送信」や「大量の無線フレームの送信」など、AP や端末における異常な振る舞いを検知して、無線 LAN サービスの性能劣化の改善につなげることができる。第 2.3.2 項で示したとおり、過去の導入事例より Beacon Flood 攻撃を検出した事例がある。攻撃を検知した場合、下図のような報告が実施される。

図 5-10　Beacon Flood 攻撃の検出事例

5.1.6　検証項目 1-6 の検証結果

(1) 検証項目の内容

適切なタイミングで Wi-Fi AP や接続されている端末を検知しているか

(2) 検証結果

リアルタイムで Wi-Fi AP や接続されている端末を検知していることを確認した。

(3) 検証内容の詳細

製品ベンダーに対するヒアリングにより、WiSAS センサーの検知タイミングはリアルタイムであるとの回答を得た。

5.1.7　検証項目 1-7 の検証結果

(1) 検証項目の内容

認可された Wi-Fi AP が登録された Wi-Fi AP ホワイトリスト、その Wi-Fi AP に接続が認可された端末が登録された端末ホワイトリストの作成は容易か

(2) 検証結果

ホワイトリストの作成は容易であることを確認した。

(3) 検証内容の詳細

実検証での検証環境構築の一環でホワイトリストの作成を実施した。Wi-Fi AP のホワイトリスト作成のためには、図 5-11 の申請書に、認可された Wi-Fi AP の MAC アドレスと SSID を記入する必要がある。

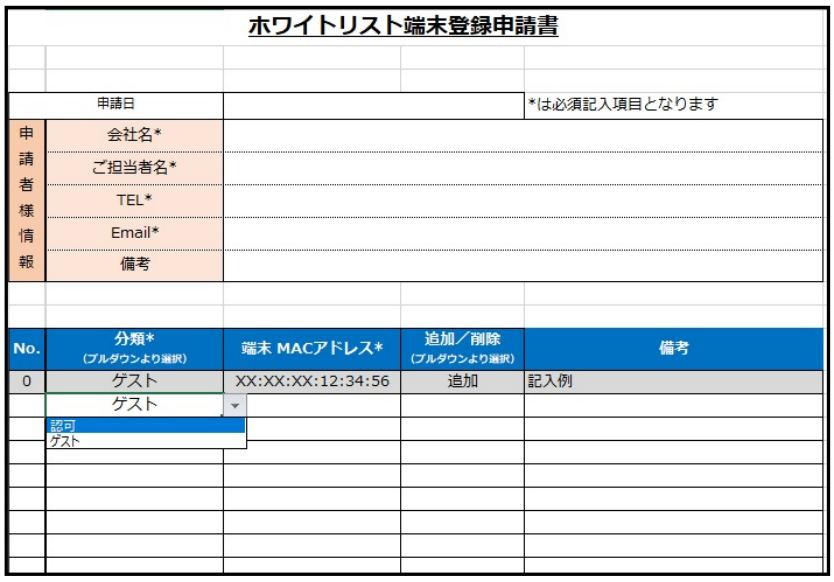
ホワイトリストAP登録申請書

申請日		*は必須記入項目となります
申請者様情報	会社名*	
	ご担当者名*	
	TEL*	
	Email*	
	備考	

No.	AP MACアドレス*	SSID*	追加／削除*（プルダウンより選	備考
0	XX:XX:XX:12:34:56	SAMPLE-WORK-WIFI	追加	記入例

図 5-11　Wi-Fi AP のホワイトリスト登録申請書

端末のホワイトリスト作成も同様であり、図 5-12 の申請書に、MAC アドレスとその端末が認可するものか、一時的なゲストかを記入する必要がある。



ホワイトリスト端末登録申請書

申請日		*は必須記入項目となります
申請者様情報	会社名*	
	ご担当者名*	
	TEL*	
	Email*	
	備考	

No.	分類* (プルダウンより選択)	端末 MACアドレス*	追加／削除 (プルダウンより選択)	備考
0	ゲスト	XX:XX:XX:12:34:56	追加	記入例
	ゲスト			
	認可			
	ゲスト			

図 5-12　端末のホワイトリスト登録申請書

いずれのホワイトリストについても、作成した申請書を管理センターへアップロードすることで登録手続きが完了する。そのため、ホワイトリストの作成は容易であると考えられる。WiSAS では検知したデバイス報告を基本としているが、ホワイトリスト／ブラックリストは一旦登録すると検知していないデバイスも一覧表として表記される（検知・未検知の識別は容易）。よって、利用者の Wi-Fi デバイスの仕分けされたデータベースとしても活用できる。なお、WiSAS は MAC アドレスで端末を識別しているため、端末のホワイトリストの登録に当たっては、ランダム MAC アドレス機能を使用しないことが強く推奨されるとのことを確認した。

5.1.8　検証項目 1-8 の検証結果

(1) 検証項目の内容

認可しない Wi-Fi AP が登録された Wi-Fi AP ブラックリスト、Wi-Fi AP に接続を認可しない端末が登録された端末ブラックリストの作成は容易か

(2) 検証結果

ブラックリストの作成は容易であることを確認した。

(3) 検証内容の詳細

第 5.1.7 項と同様に、実検証での検証環境構築の一環でブラックリストの作成を実施した。ブラックリスト作成も第 5.1.7 項と同様であり、図 5-11 及び図 5-12 と同様の内容である「ブラックリスト AP 登録申請書」、「ブラックリスト端末登録書」に記入し、その申請書を管理センターへアップロードすることで登録手続きが完了する。そのため、ブラックリストの作成は容易であると考えられる。

5.1.9　検証項目 1-9 の検証結果

(1) 検証項目の内容

一時利用と常時設置 Wi-Fi AP の識別は容易か

(2) 検証結果

一時利用と常時設置 Wi-Fi AP の識別は容易であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS NORA（常時監視サービス）を 3 日間の期間で導入し、その結果を示す報告書により、ホワイトリストにない Wi-Fi AP を検知した場合どのように識別されているか確認した。一次利用 AP の検知結果と常時設置 Wi-Fi AP の検知結果をそれぞれ図 5-13 及び図 5-14 に示す。それぞれの区分で Wi-Fi AP の MAC アドレス、当該 Wi-Fi AP のベンダー、SSID、SSID 分類等が出力されるため、一時利用と常時設置 Wi-Fi AP の識別は容易に実施できる。

図 5-13　一時利用 AP の検知結果

WiSAS

Spline Network

Confidential

B-1 常時設置APの一覧

この項目のポイント

WiSASセンサーが設置されている拠点において、未確認の無線APが常時設置されていることを示す一覧です。
常時設置APが検知された場合、機密情報が外部に持ち出されるリスクがあります。
さらに、「端末接続有無」が「あり」の場合、常時設置APに端末が接続されて情報が流出している可能性があるため、早急に対処が必要となります。
常時設置APに接続している端末の詳細な情報は「B-2 常時設置APへの端末接続履歴」に記載されています。
また、検知後の対応として「位置情報検知オプション」による常時設置APの位置特定、並びに常時設置APの撤去による恒久対策を推奨いたします。

結果	検知台数
常時設置APが検知されました。	10台

分類	AP MAC	ベンダー	SSID	SSID分類	認証	暗号化	プロトコル	チャンネル	dBm	端末接続有無
外部				公開	WPA2-PSK	AES-CCMP	b/g/n	5	-54	あり
外部				公開	WPA2-PSK	AES-CCMP	a/n	48	-58	あり
外部				公開	WPA-PSK/WPA2-PSK	AES-CCMP	b/g/n	2	-63	あり
外部				公開	WPA-PSK/WPA2-PSK	TKIP-AES-CCMP	b/g/n	6	-65	あり
外部				公開	WPA2-PSK	AES-CCMP	b/g/n	11	-65	なし
外部				公開	WPA2-PSK	AES-CCMP	a/n	108	-65	なし
外部				公開	WPA-PSK/WPA2-PSK	TKIP-AES-CCMP	b/g/n	8	-66	なし
外部				公開	WPA2-PSK	AES-CCMP	b/g/n	1	-66	あり
外部				公開	WPA2-PSK	AES-CCMP	ac	56	-68	あり
外部				公開	WPA2-PSK	AES-CCMP	b/g/n	6	-68	なし

図 5-14　常時設置 AP の検知結果

5.1.10　検証項目 1-10 の検証結果

(1) 検証項目の内容

一時利用と常時設置 Wi-Fi AP に接続した端末の識別は容易か

(2) 検証結果

一時利用と常時設置 Wi-Fi AP に接続した端末の識別は容易であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS NORA（常時監視サービス）を 3 日間の期間で導入し、その結果を示す報告書により、ホワイトリストにない Wi-Fi AP に接続した端末がどのように識別されているか確認した。一次利用 AP への端末接続履歴と常時設置 AP への端末接続履歴の結果をそれぞれ図 5-15 及び図 5-16 に示す。それぞれの区分で、接続された Wi-Fi AP の MAC アドレス、SSID、接続した端末の MAC アドレス、端末のベンダー、接続時間、開始時間及び終了時間が出力されるため、一時利用と常時設置 Wi-Fi AP への端末接続の識別は容易に実施できる。

図 5-15　一時利用 AP への端末接続の検知結果

図 5-16　常時設置 AP への端末接続の検知結果

5.1.11　検証項目 1-11 の検証結果

(1) 検証項目の内容

通知は適切な手段でリアルタイムに実施されるか

(2) 検証結果

通知はメールにて、リアルタイムで実施されることを確認した。

(3) 検証内容の詳細

実検証により確認した。図 5-1、図 5-4、図 5-7 に示すとおり、認可されていない Wi-Fi AP と同じ SSID になりすました AP が検知・遮断された場合、認可されている Wi-Fi AP に対して認可されていない端末が接続して検知・遮断された場合、そして Wi-Fi Direct 機能が有効にされているプリンターに対して認可されていない端末が Wi-Fi Direct 機器に接続され、それを検知・遮断した場合に、リアルタイムでメールが受信できることを確認した。

5.1.12 検証項目 1-12 の検証結果

(1) 検証項目の内容

現状の AP／端末リスト及び不正な AP／端末リストの表示仕様は分かり易いか

(2) 検証結果

現状の AP／端末リスト及び不正な AP／端末リストの表示仕様は分かり易いことを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。WiSAS 環境スキャンのサービスを実施し、現状の Wi-Fi AP 及び端末の確認を行った。スキャンの結果は報告書にて図 5-17 及び図 5-18 のとおり示された。Wi-Fi AP 一覧では、スキャンによって特定された AP の MAC アドレス、SSID、SSID 分類等が一覧で確認できる。また、端末一覧では、端末の MAC アドレスとその端末が接続した Wi-Fi AP の MAC アドレス及び SSID 等を一覧で確認できる。なお、常時監視ソリューションでは接続情報に、接続開始時間と接続終了時間をも報告される。不正な AP／端末リストについても、第 5.1.1 項及び第 5.1.2 項で示したとおり不正な AP／端末を一覧で確認することができる。以上より、現状の AP／端末リスト及び不正な AP／端末リストの表示仕様は分かり易いと判断した。

WiSAS

Spline Network

Confidential

WiSAS 環境スキャン

AP一覧

AP MAC	SSID	SSID分類	認証	暗号化	プロトコル	チャンネル	dBm
[redacted]		公開	WPA2-PSK	AES_CCMP	b/g/n	11	-28
		公開	WPA2-PSK	AES_CCMP	ac	100	-30
		公開	WPA2-PSK	AES_CCMP	b/g/n	11	-31
		公開	WPA2-PSK	AES_CCMP	ac	100	-32
		公開	WPA2-PSK	AES_CCMP	ac	100	-33
		公開	WPA2-PSK	AES_CCMP	b/g/n	11	-33
		公開	WPA2-PSK	AES_CCMP	g/n	3	-37
		公開	WPA2-PSK	AES_CCMP	b/g/n	5	-51
		公開	WPA2-PSK	AES_CCMP	a/n	48	-54
		公開	WPA-PSK/WPA2-PSK	TKIP_AES_CCMP	b/g/n	8	-57

図 5-17　WiSAS 環境スキャンによる AP 一覧

WiSAS

Spline Network

Confidential

WiSAS 環境スキャン

端末一覧

端末MAC	接続AP MAC	接続AP SSID	dBm
[redacted]			-72
			-75
			-80
			-81
			-81
			-82
			-87
			-88
			-88
			-89
			-89
			-89
			-99

図 5-18　WiSAS 環境スキャンによる端末一覧

5.1.13　検証項目 1-13 の検証結果

(1) 検証項目の内容

報告書は読み易いか

(2) 検証結果

今回の実検証で確認した以下の 4 つのサービス全てにおいて、読み易い報告書が提示さ

れることを確認した。

- WiSAS 環境スキャン
- WiSAS 脆弱性診断
- WiSAS NORA（常時監視ソリューション）
- WiSAS 24H365D（常時監視ソリューション）

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。

まず、WiSAS 環境スキャンの報告書について、第 5.1.12 項で示したとおり現状の Wi-Fi AP 及び端末を一覧として把握できることを確認した。

WiSAS 脆弱性診断の報告書は、診断の実施概要がまず記載され、その後結果サマリ、詳細結果、検出されたデバイス一覧が記載される。結果サマリでは、以下の 6 つの項目に基づく診断結果を定量的に確認することができる。

- 非認可端末：認可された Wi-Fi AP へ接続した、非認可端末の存在
- 不正行為端末：認可されていない Wi-Fi AP へ接続した、認可端末の存在
- なりすまし AP：SSID が同じ、なりすまし Wi-Fi AP の存在
- MAC 偽装 AP：認可された Wi-Fi AP に MAC アドレスを偽装した Wi-Fi AP の存在
- Wi-Fi Direct AP：Wi-Fi Direct の電波を送出している Wi-Fi AP の存在
- ハッキングデバイス：悪意あるハッキングデバイスの存在

WiSAS 脆弱性診断の報告書における結果サマリを図 5-19 に示すとおりであり、それぞれの項目における検知件数・危険度を踏まえた総合評価を直ぐに確認することができる。

WiSAS　　Spline Network

Confidential

B. 結果サマリ

総合評価

評価	概要
D	深刻な脆弱性あり

評価基準

評価	概要	説明
A	異常なし	危険なWi-Fiの利用が検知されなかった。
B	軽微な脆弱性あり	危険度(低)を検知。時間の経過によりセキュリティ被害につながる可能性があるため、注意が必要。
C	検討を要する脆弱性あり	危険度(中)を検知。セキュリティ被害につながる可能性があり、対応の検討が必要。
D	深刻な脆弱性あり	危険度(高)を検知。セキュリティ被害を受けている可能性があり、早急に対応が必要。

項目別件数

項目	説明	危険度	検知件数
非認可端末			
認可AP外部端末接続	外部端末が内部の認可されたAPに接続している場合	高	3
認可AP未分類端末接続	未分類端末が内部の認可されたAPに接続している場合	高	10
不正行為端末			
外部AP認可端末接続	認可端末が外部APに接続している場合	中	34
未分類AP認可端末接続	認可端末が未分類APに接続している場合	低	4
ゲストAP認可端末接続	認可端末がゲストAPに接続している場合	低	0
なりすましAP			
なりすましAP探知	非認可APが社内の認可APと同じSSIDを使用している場合	中	2
なりすましAP認可端末接続	認可端末がなりすましAPに接続している場合	高	0
MAC偽装AP			
AP MAC偽装探知	認可APのMAC addressがSpoofingされた場合	中	0
AP MAC偽装認可端末接続	認可端末がMAC偽装 APに接続している場合	高	0
WI-FI Direct AP			
Wi-Fi Direct AP探知	Wi-Fi Direct APが探知された場合	低	161
Wi-Fi Direct AP端末接続	端末がWi-Fi Direct APに接続している場合	中	22
ハッキングデバイス			
ハッキングデバイス探知	ハッキングデバイスが探知された場合	低	0
認可APハッキングデバイス接続	ハッキングデバイスが認可APに接続している場合	中	0
ゲストAPハッキングデバイス接続	ハッキングデバイスがゲストAPに接続している場合	中	0

図 5-19　WiSAS 脆弱性診断サービスの報告書における結果サマリ

また、詳細結果にはそれぞれの項目におけるポイント、診断結果、検出・遮断件数、イベント一覧が記され、検知・遮断された Wi-Fi AP や端末に関する情報を詳細に確認することができる。

WiSAS NORA（常時監視ソリューション）及び WiSAS 24H365D（常時監視ソリューション）の報告書も同様の構成であり、まず結果サマリが記載された後、詳細結果が記載される。結果サマリは図 5-19 の形式で示されるため、それぞれの項目における検知件数・危険度を踏まえた総合評価を直ぐに確認することができる。詳細結果についても同様でありそれぞれの項目におけるポイント、診断結果、検出・遮断件数、接続開始時間・接続終了時間、結果一覧が記され、検知・遮断された Wi-Fi AP や端末に関する情報を詳細に確認することができる。

以上より、4 つのサービス全てにおいて、読み易い報告書であると判断した。

5.1.14　検証項目 1-14 の検証結果

(1) 検証項目の内容

報告書の内容は不正 Wi-Fi AP の持ち込み、端末の不正接続の対策として有用な情報が記載されているか

(2) 検証結果

報告書には、不正 Wi-Fi AP の持ち込み、端末の不正接続の対策として有用な情報が記載されていることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び検証の結果提示される報告書に基づき評価した。図 5-2 や図 5-5 に示すとおり、報告書の詳細結果の項目では、それぞれの項目ごとに「この項目のポイント」の枠が存在し、その中で対策として有用な情報が記載されている。例えば、「なりすまし AP」に関する項目であれば、「なりすまし AP に誤って認可端末が接続した場合、通信を傍受されたり、重要な情報が盗まれたり、認可端末を乗っ取られる危険性があります。もしこの項目が検知された場合、位置情報分析オプションによる、なりすまし AP の位置特定と撤去を推奨いたします。」といった内容が記載され、なりすまし AP が見つかった場合の危険性と、それに対する対応策が示されている。

以上より、報告書には、不正 Wi-Fi AP の持ち込み、端末の不正接続の対策として有用な情報が記載されていると判断した。

5.2　運用性に関する検証結果

5.2.1　検証項目 2-1 の検証結果

(1) 検証項目の内容

障害時の復旧対応は準備されているか

(2) 検証結果

障害時の復旧対応が準備されていることを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーへのヒアリングにより確認した。障害時の復旧対応に関して、基本サービスでは NTT docomo の LTE 回線を使用しているため、回線の状況には関与できないとのことであった。また、WiSAS センサーの死活監視は、アラートメール、日々の管理サーバーチェックにて行っており、異常が見られた場合には、あらかじめ登録された担当者へエスカレーションすることになっているとの回答を得た。万が一、WiSAS センサー自体に異常があった場合は、直ぐに代替品を利用者に届ける仕組みとなっているとのことで

あった。なお、データセンターの管理サーバー及びアーカイブサーバーは、十分な冗長性を確保し、その他、障害時対応に関しては、WiSAS サービス仕様書（常時監視）、WiSAS SLA を用意しており、障害時対応については万全を期しているとのことであった。

5.2.2　検証項目 2-2 の検証結果

(1) 検証項目の内容

当該サービスの活用方法を容易に習得できるか

(2) 検証結果

サービスの活用方法を容易に習得できることを確認した。

(3) 検証内容の詳細

利用者におけるサービスの習得性については、実検証及び検証の結果提示される報告書に基づき評価した。上述のとおり、WiSAS センサーは適切な箇所に配置し電源につなげるだけでサービスを利用することができるため、利用方法の習得は必要ない。また、診断結果を確認する報告書についても詳細な解説と必要な情報が記載してあり、Wi-Fi セキュリティを担保する上でのホワイト／ブラック／未確認の概念を理解し、適宜必要なサービスを適用することができる。

なお、販売代理店を対象とした Wi-Fi セキュリティポリシーと教育プログラムを制作中であることをヒアリングにより確認した。

5.2.3　検証項目 2-3 の検証結果

(1) 検証項目の内容

今後の事業方針・目標は明確か

(2) 検証結果

明確な事業方針や目標が定められていることを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーへのヒアリングにより確認した。WiSAS はセキュリティ製品ゆえに継続率は高いと想定され、サブスクリプション方式ゆえに導入がしやすく、売上が積み上っていくストック型のビジネスのモデルであり、ビジネスプランとして 5 年後には 10 億の売上を計画しているとのことであった。現状で 10 社近くの大手 SIer、監査機関、ネットワーク事業者、デジタルフォレンジック調査会社等が代理店になっているとのことであった。

5.2.4　検証項目 2-4 の検証結果

(1) 検証項目の内容

製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか

(2) 検証結果

安価なサービス提供、サービスの拡大、海外進出等を予定しているとのことであった。

(3) 検証内容の詳細

本検証項目は製品ベンダーへのヒアリングにより確認した。新型コロナウイルス感染症拡大の影響を踏まえ、テレワークや個人宅向けの安価なサービスを検討しているとのことであった。また、図 5-3 等で示される、認可されていない Wi-Fi AP や端末の位置特定に関して、現状では位置の特定は即時的に実施されるものの、利用者への正式な通知は報告書を介して実施されるため数日後に通知される形となる。このタイムラグに対して、実際の現場では位置を特定できた段階で利用者に連絡するサービス形態で運用しているとのことであった。また、複数の利用者から海外事務所での利用相談を受けており、知財戦略（特許）含め市場拡大を計画しているとのことであった。

現状のところ他社製品との連携予定はないが、複数の SIer が他社有線ネットワーク製品と組み合わせた統合セキュリティサービスとして展開しているとのことであった。

5.3　導入容易性に関する検証結果

5.3.1　検証項目 3-1 の検証結果

(1) 検証項目の内容

短時間で導入できるか

(2) 検証結果

実検証により、設置自体は数分程度で完了することを確認した。

(3) 検証内容の詳細

実際の検証環境（図 4-1）に WiSAS センサーを設置することで確認を行った。WiSAS センサー一式は図 5-20 に示すとおり、センサー本体、電源アダプタ、電源ケーブル、マウントキット（申込者のみ）、及びセンサー取扱マニュアルによって構成される。

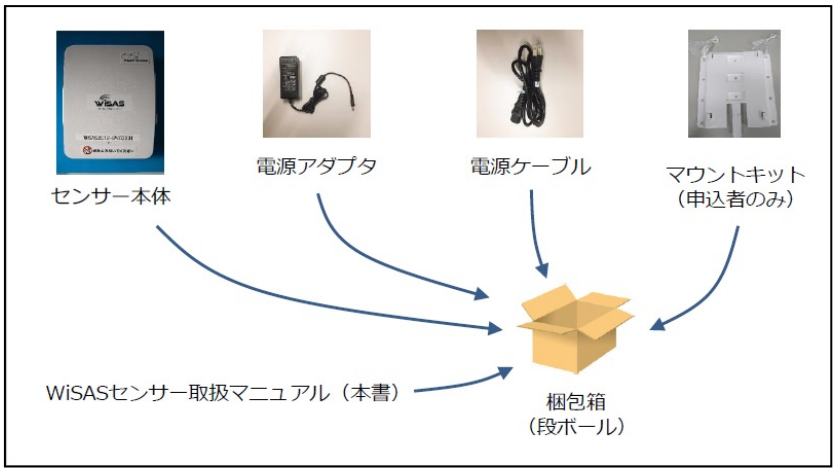


図 5-20　WiSAS センサー・付属品一式

WiSAS センサー及び付属品を受領した後、設置場所を検討する必要がある。WiSAS センサーは電波を利用するため、設置環境が探知の精度に大きく影響するため、設置位置を決める際は以下の点に配慮する必要がある。

＜設置位置を決める際に配慮すべき点＞

- 干渉波（電子レンジ、モーター等）
- 遮蔽物（壁、パーティション、柱、キャビネット等）
- 建物の構造（閉鎖／吹き抜け）
- 設備の材質（鉄、コンクリート、木材等）
- 対象となる現場の設備状況（ラックや棚などの設備状況）
- 高所（高所は遮蔽物の影響を受けづらいため）
- 中央（カバーエリアを考慮）

なお、位置情報分析サービスを利用するためには、3 台以上の WiSAS センサーをグループ化して同一フロアに設置する必要がある。理想的なセンサー配置のイメージを以下の図 5-21 に示す。基本的にセンサーの数が密であるほど検知精度は向上するものの、電波干渉要因は多種多様であるため、その現地特有の要因により、検知精度は左右されるとのことであった。

図 5-21　WiSAS センサーの理想的な配置方法

上記の観点を踏まえて、図 4-2 のとおり 3 箇所にセンサーを配置した。センサー自体は電源につなげるだけで起動し、その後 1 分程度で管理センターに接続したため、全体を通じて 5 分程度で設置が完了した。

5.3.2　検証項目 3-2 の検証結果

(1) 検証項目の内容

作業は 1 人で可能か

(2) 検証結果

WiSAS センサーの設置は 1 人で十分可能であることを確認した。

(3) 検証内容の詳細

第 5.3.1 項に示したとおり、実際の環境に設置することで確認した。

5.3.3　検証項目 3-3 の検証結果

(1) 検証項目の内容

別途必要となる費用は発生するか

(2) 検証結果

別途必要となる費用は発生しないことを確認した。
なお、製品ベンダーではセンサー設置を請け負うサービスも用意している。

(3) 検証内容の詳細

第 5.3.1 項に示したとおり、実際の環境に設置することで確認した。

5.3.4　検証項目 3-4 の検証結果

(1) 検証項目の内容

用意が必要となる機器はあるか

(2) 検証結果

コンセントから 3m 以上離れた位置に WiSAS センサーを設置する場合には、テーブルタップ等が必要であることを確認した。その他用意が必要となる機器はないことを確認した。

(3) 検証内容の詳細

第 5.3.1 項に示したとおり、実際の環境に設置することで確認した。WiSAS センサーを動作させるためには電源ケーブルをコンセントに接続する必要があるが、付属ケーブルを合わせた長さが 3m のためコンセントまでの距離がそれ以上の場合はテーブルタップが必要である。

5.3.5　検証項目 3-5 の検証結果

(1) 検証項目の内容

安全性や機密性に問題はないか

(2) 検証結果

安全性や機密性に特段の問題がないと考えられることを確認した。

(3) 検証内容の詳細

仕様書の確認及び製品ベンダーに対するヒアリングによって確認した。WiSAS の構成要素について以下の安全性・機密性に対する対応を行っていることを確認した。

- 管理センター：
  日本国内のデータセンターを利用している。ISMS クラウドセキュリティ認証取得組織の環境を利用し、特定の送信元グローバル IP アドレスの通信しか受け付けないようアクセス制限されている。さらに、四半期に一度の定期で外部の専門業者によるセキュリティ検査を実施し、セキュリティを確保している。
- WiSAS センサーと管理センター間の通信：
  WiSAS センサーと管理センター間の通信は暗号化されており、WiSAS センサーは IEEE802.11 フレームのヘッダ部のみを監視しているため、IP アドレスやアプリケーション等のデータ部に関する情報は監視しておらず、触れることはない。WiSAS センサーには Wi-Fi AP の機能はなく、唯一遮断時に強制切断メッセージを送信するだけである。
- アーカイブサーバー：
  実績あるクラウドストレージサービスを活用している。アップされたデータは細

分され、それぞれのファイルを暗号化することでセキュリティを担保している。URL は非公開で、閲覧権限のあるパスワードは退職者や担当者変更に備え、利用者自身で任意に変更可能である。

- WiSAS センサー：
  WiSAS センサー本体は技適マーク、電源アダプタは PSE マークを取得しており安全性において問題はない。

また、WiSAS 関連機器の設計製造時に各種耐久試験やエージング試験を実施していることを確認した。WiSAS センサーが取得するデータは Wi-Fi ヘッダ情報のみで、通信データは監視しておらず、データをアップロード及び管理するクラウドも機密性は問題ないと考えられる。また、WiSAS センサー本体の安全性も問題ないと考えられる。

6. まとめ

WiSAS は、Wi-Fi 環境のセキュリティを担保するために調査・監視するセキュリティソリューションであり、Wi-Fi 環境を安全に使用するための可視化や分析を行い、不正利用やサイバー攻撃による情報漏洩を防止する機能を提供する。昨今の Wi-Fi 環境を取り巻く環境を踏まえると、Wi-Fi 環境のセキュリティ対策の重要性はより高まっていくと考えられるが、WiSAS は既存のシステムを変更することなく、手軽に短期間で導入することが可能である。また、復旧を除く運用時も利用者の手を煩わせない点が特徴として挙げられる。

今回の検証は、前述の検証環境、検証条件、方法の範囲で、WiSAS の 4 つの差別化ポイントとされている事項に対して、「製品機能・性能」、「運用性」、「導入容易性」の観点から検証を実施し確認した。

セキュリティ製品の有効性検証の検証結果について

株式会社グレスアベイル
「GUARDIAX SaaS 版」

目 次

図 目 次

表 目 次

用語集・略語集

本報告書では、以下のとおり用語を定義する。

用語	概要
AWS	Amazon Web Services の略。
Apache Struts	Web アプリケーションを開発するためのフレームワークをいう。
Burp Suite	脆弱性診断に使われるローカルプロキシツールをいう。
CGI	Common Gateway Interface の略で、Web サーバーが、Web ブラウザなどからの要求に応じてプログラムを実行する仕組みをいう。
EC-CUBE	オープンソースの EC サイト向けコンテンツ管理システムをいう。
FQDN	Fully Qualified Domain Name の略で、インターネット等におけるドメイン名の表記法の一つで、トップレベルドメインから順番に、サブドメイン名やホスト名など各階層を省略せずにすべて指定した形式をいう。
HTTP	Hyper Text Transfer Protocol の略で、Web サーバーと Web クライアントの間でデータの送受信を行うために用いられる通信規約をいう。
IIS	Internet Information Services の略で、Windows Server シリーズに同梱されている Web サーバーソフトウェアをいう。
IP	Internet Protocol の略で、複数の通信ネットワークを相互に接続し、データを中継・伝送して一つの大きなネットワークにすることができる通信規約をいう。
Java	オブジェクト指向プログラミング言語をいう。
LDAP	インターネットなどの TCP/IP ネットワークでディレクトリサービスにアクセスするための通信プロトコルをいう。
OS	Operating System の略で、ソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアをいう。
OS コマンド	コンピュータの利用者が OS のシェルに与える文字列による命令をいう。
PHP	Web サーバーの機能を拡張し、動的に Web ページを生成するために用いられるプログラミング言語をいう。
SIRT	Security Incident Response Team の略で、企業や行政機関などに設置される組織の一種で、コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織をいう。
SQL	リレーショナルデータベース（RDB : Relational Database）の管理や操作を行うための問い合わせ言語をいう。
UI	User Interface の略で、システムから利用者への情報の提示・表示の仕方と、利用者がシステムを操作したり情報を入力したりする手段や方式、機器、使い勝手をいう。

用語	概要
Web アプリケーション	Web ページと共通の技術を応用して構築・運用されるアプリケーションソフトをいう。
インジェクション	ソフトウェアへの攻撃手法の一つで、外部から文字列の入力を受け付けるプログラムに対して開発者の想定外の不正な文字列を与え、システムを乗っ取ったり、データの改竄や詐取を行ったりする手法をいう。
クラウド	インターネット等のネットワーク経由で、ユーザーにサービスを提供する形態をいう。
クロスサイト・スクリプティング	利用者が入力した内容を表示するような構成の Web サイトに存在する欠陥を悪用して、攻撃者が用意した悪意のあるスクリプトを利用者の元に送り込んで実行させる攻撃をいう。
シグネチャ	コンピュータウイルスなどに含まれる特徴的なデータ断片や攻撃者のアクセスに特徴的な受信データのパターンなどをいう。
ダッシュボード	複数の情報源からデータを集め、概要をまとめて一覧表示する機能や画面、ソフトウェアなどをいう。
ディレクトリ	ディレクトリの中にサブディレクトリを作成し、その中にさらにファイルやディレクトリを作ることができ、全体を階層構造で表すことができるものをいう。
ファイルインクルード	プログラムの中で別ファイルを参照するコードがあった場合、実際に参照すべきファイルとは別のファイルやデータを読み込ませ、本来意図しない不正なデータ処理を行わせる攻撃をいう。
ブルートフォースアタック	割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、検証する方式をいう。
ミドルウェア	ソフトウェアの種類の一つで、OS とアプリケーションソフトの中間に位置し、様々なソフトウェアから共通して利用される機能を提供するものをいう。
改行コード	テキストデータ中で、改行を指示する特殊な文字コード（改行コード）、及び改行を表す特殊文字（改行文字）をいう。

1. はじめに

経済産業省の産業サイバーセキュリティ研究会 WG3（サイバーセキュリティビジネス化）は、信頼できるセキュリティ製品と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている。具体的には、日本で開発されたセキュリティ製品について有効性検証・実環境における試行導入を実施しその結果を発信することで、ユーザーが、日本で開発された製品を選定しやすい環境を構築するものである。

独立行政法人情報処理推進機構（以下「IPA」という。）は、経済産業省の委託を請け、2019 年 9 月にこの事業のあり方を検討する「サイバーセキュリティ検証基盤構築に向けた有識者会議」を設置した。有識者会議の検討において、検証基盤の対象製品を日本発のスタートアップ製品とし、効率的な有効性検証の仕組みとして具体化すること、また今年度は「脅威の可視化」、「脆弱性の可視化」、「IT 資産の認証／検証」に係る製品分野を検証対象とすることを方針とした。

本報告書は、本基盤を試行運用して、検証対象候補の製品を公募しその中から対象製品を選定して有効性検証を行った結果を報告するものである。特に、専門家による客観的な「セキュリティ製品の有効性検証」について今年度は 2 製品を選定して、試行的な検証の題材とし、IPA が事務局となって実際に試行検証を実施した。

以下では、株式会社グレスアベイルの「GUARDIAX SaaS 版」を対象に実施した有効性検証の検証結果について示す。

2. 検証対象製品 GUARDIAX SaaS 版について

2.1 対象製品を取り巻く環境

IPA 発行の情報セキュリティ白書 2020 に記載されているように、2019 年度のセキュリティの概況では、2019 年 5 月に EC サイトのアカウント 46 万 1,000 件に不正アクセス、アンケートモニターサービスの登録アカウント 77 万 74 件に不正アクセスなど、Web サイト（サービス）への不正アクセスは現在でも行われている。不正アクセスから Web サイトやサービスを守る手段の一つとして Web Application Firewall（WAF）があり、WAF を導入するきっかけとして次の 3 つの例が想定される。

- 例 1 : Web サイトに脆弱性が潜在している可能性を懸念して、不正アクセスによる脅威から Web サイトを守るために当初から WAF を導入する。
- 例 2 : Web サイトが不正アクセスを受けていることが発覚し、その対応のために Web アプリケーションを改修するまでの間、不正アクセスから Web サイトを守るために WAF を導入する。
- 例 3 : Web アプリケーションで使用しているミドルウェアに脆弱性が発見されたという情報を確認したので、その脆弱性を狙った不正アクセスから Web サイトを守るために WAF を導入する。

2.2 製品概要

GUARDIAX は、サイバー攻撃から Web アプリケーションを守るための WAF 製品である。本製品は SaaS 版とコンテナ版の 2 方式が準備されているが、今回の検証では SaaS 版を対象とした。

図 2-1　GUARDIAX SaaS 版の概要

グレスアベイル社は、本製品の特徴として以下の 5 点を挙げている。

- **過検知、誤検知が劇的に減少**：
  GUARDIAX は WAF の防御範囲である不正ログイン試行、Web アプリケーションの脆弱性への攻撃などをブロックするだけでなく、これまでの WAF の課題であった過検知や誤検知を劇的に減少させている。当製品は、Web アプリケーションセキュリティの第一人者である徳丸浩氏がシグネチャを監修しており、防御ルールを明確化させるなどの試行錯誤のもと、高検知率を誇るサービスを実現している。
- **個人情報保護機能の搭載**：

マイナンバーやクレジットカード番号といった、個人情報の流出を防ぐ保護機能を搭載している。これは Web サーバーから送信されるデータを監視し、流出を検知・ブロックする仕組みであり、攻撃者による個人情報窃取、正規利用者の誤操作による個人情報のアップロードといった双方向のリスクを防御する。

- **自社開発による低コスト実現：**
  グレスアベイルの自社開発によって提供する GUARDIAX は、月額 1 万円からという低コストを実現している。コンテナ技術の活用により、OS やライブラリなどの動作環境に依存することを回避し、開発コストが抑えられたことによって、低コストでの提供が可能となった。
- **簡単で身近な SaaS 版提供：**
  通信に対するセキュリティをクラウド上に配した SaaS 版での提供が可能である。自社内に多数の機器を設置する必要がなく、インターネットに繋がる環境であれば低コストかつスピーディに導入・運用ができる。社内のシステム環境などによって違いはあるが、最短 24 時間以内に導入が可能である。
- **一覧性、操作性に優れた UI：**
  ダッシュボードは現在の攻撃状況やログ、統計などが一目瞭然であるほか、ユーザー向けマニュアルを用意しており、誰でも簡単に対応することができる。一つ一つのサイトにきめ細かく設定することもでき、迅速かつ適切なセルフ管理が可能である。また、ログ情報や統計情報はレポーティングできるので、自社の運用管理を飛躍的に向上することが可能となる。

2.3 製品の導入事例

2.3.1 大手鉄道会社での導入事例

大手鉄道会社における SIRT 主導の下、グループ傘下各社に対して WAF を展開することとなった。グループ内に存在する多くのサイトを、サイト毎の特性に合わせてルールのチューニングを行いたいという要望があり、本製品が採用された。

3. 検証する差別化ポイント・検証項目

3.1 検証する対象の差別化ポイントとされる事項

GUARDIAX SaaS 版（以下、「GUARDIAX」という。）の差別化ポイントとされる事項のうち、本検証では以下の 4 つの事項に対して検証を実施した。

(1) **強固な防御ルールであること**
Web アプリケーションの脆弱性を利用した攻撃に対する防御ルールが強固である。

(2) **偽陽性が少ないこと**
偽陽性(正常なアクセスを誤って防御してしまう)が少ないため、短期間(最短 1 日)での導入や利便性の高い運用が可能である。

(3) **攻撃状況が判るダッシュボードが用意されていること**
WAF のダッシュボードにより攻撃（不正アクセス）の状況が判る。

(4) **防御ルールを Web サイト単位でチューニングできること**
Web サイト毎にチューニングした防御ルールを設定できる。

3.2 検証項目

本検証基盤では、重要分野に共通して適用される検証項目の大分類を策定し、それぞれの大分類の下に選定された各製品の個別検証項目を策定する形式とした。今年度の有効性検証においては、重要分野に共通して適用される大分類を「製品機能・性能」、「運用性」、「導入容易性」の 3 つとした。

3.2.1 製品機能・性能に関する検証項目

GUARDIAX の差別化ポイントとされる事項を踏まえ、製品機能・性能に関して、表 3-1 に示す検証項目について検証した。

表 3-1 製品機能・性能に関する検証項目

No.	区分	検証項目
1-1	防御	強固な防御ルールを実現できているか
1-2		偽陽性が少ないか
1-3		SaaS 版とコンテナ版に性能の差異は存在しないか
1-4	ダッシュボード	ダッシュボードにおいて攻撃の有無を確認できるか
1-5		ダッシュボードにおいて検知した攻撃の詳細を確認できるか
1-6		ダッシュボードにおいて検知した攻撃のレベル分けができるか
1-7		ダッシュボードにおいて Web サイトの脆弱性を指摘するか

3.2.2 運用性に関する検証項目

GUARDIAX の差別化ポイントとされる事項を踏まえ、運用性に関して、表 3-2 に示す検証項目について検証した。

表 3-2　運用性に関する検証項目

No.	区分	検証項目
2-1	防御ルールの設定	防御ルールの設定変更の反映のタイミングを設定できるか
2-2	ダッシュボード	攻撃情報は分かり易いか
2-3		ログ分析は分かり易いか
2-4		防御ルールの更新連絡は存在するか
2-5	対故障性	障害時の復旧対応が準備されているか
2-6	習得容易性	当該製品の活用方法を容易に習得できるか
2-7	提供の継続性	今後の事業方針・目標は明確か
2-8	拡張性・他製品との連携の可能性	製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか

3.2.3　導入容易性に関する検証項目

GUARDIAX の差別化ポイントとされる事項を踏まえ、導入容易性に関して、表 3-3 に示す検証項目について検証した。

表 3-3　導入容易性に関する検証項目

No.	区分	検証項目
3-1	導入の容易性	導入する Web サイトやサーバーに制約条件はあるか
3-2		導入に至るまでの手続きは簡単か
3-3		導入時の設定は簡単か
3-4		導入に当たってサービスの停止が必要か
3-5		Web アプリケーションに対する変更が必要か
3-6		導入までの必要期間は短期間か
3-7	安全性・機密性	安全性や機密性に問題はないか

4. 検証環境・検証条件

4.1 検証環境の構築

図 4-1 に示すとおり、AWS にテスト用の Web サイト（hacker.jp）を構築し、GUARDIAX SaaS 版を経由してアクセスする環境を構築した。

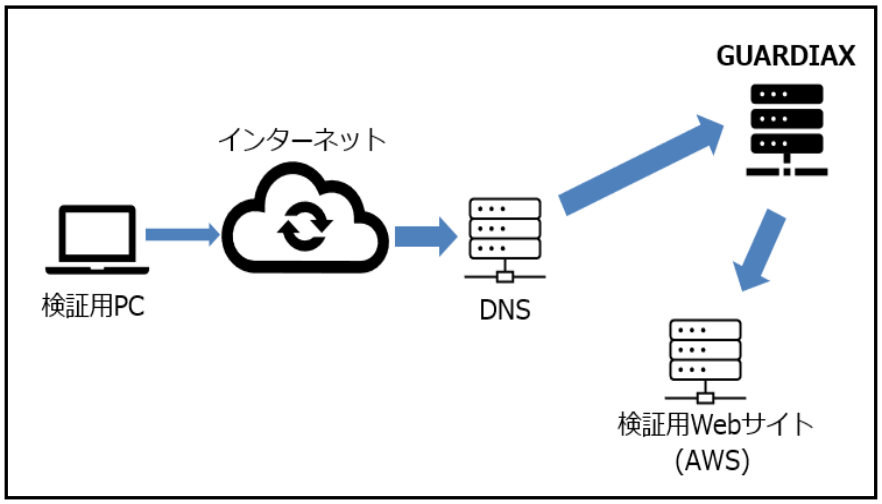


図 4-1 検証環境

GUARDIAX SaaS 版の利用に当たって、まず GUARDIAX 申請書を作成しアカウント情報が提供された後、ダッシュボードにて検証用 Web サイトの FQDN を登録した。その後、ダッシュボードにて防御ルールを設定した。

4.2 検証条件

検証用 Web サイト（AWS）は GUARDIAX からのアクセスのみを IP 制限により許可した。また、防御機能を確認するために、以下に示す通信（HTTP リクエストまたはレスポンス）を一つ以上発生させ、防御機能の有効性や、ダッシュボードにおける表示を検証した。

- スキャニング検出
- クロスサイト・スクリプティング (XSS)
- SQL インジェクション
- OS コマンド・インジェクション
- PHP インジェクション
- 改行コードインジェクション
- LDAP インジェクション
- ローカルファイルインクルード
- リモートファイルインクルード
- Java 攻撃
- Apache Struts2 攻撃
- ブルートフォースアタック
- EC-CUBE 攻撃
- クレジットカード情報データ

- SQL エラー
- Java 情報
- PHP 情報
- IIS 情報
- ディレクトリ情報
- CGI 情報

ブルートフォースアタックについては SaaS 版 GUARDIAX のルール設定画面には存在しなかったが、登録した Web サイト毎に単一 IP からのリクエスト数を制限する機能が存在したため、これをブルートフォースアタックに対する防御機能として記載する。この機能によって制限されたアクセスは、ダッシュボード上では「アクセス制御」の攻撃種別として表示される。なお、攻撃はプロキシツールである Burp Suite を用いて実施した。

また、検証する差別化ポイントとされる事項のうち「強固な防御ルール」及び「偽陽性が少ない」については、OWASP が発行している Web アプリケーションセキュリティに関するレポートである OWASP Top 10（2017）に基づいてグレスアベイル社が実施した検証結果と、その結果を参考に実検証した結果に基づき評価を行った。

5. 検証結果

5.1 製品機能・性能に関する検証結果

5.1.1 検証項目 1-1 の検証結果

(1) 検証項目の内容

強固な防御ルールを実現できているか

(2) 検証結果

製品ベンダーから提供されたデータに基づいて、強固な防御ルールを実現していることを確認した。

(3) 検証内容の詳細

実検証及び製品ベンダーによるデータや記録に基づき評価を行った。まず、OWASP Top 10 で提示された Web アプリケーションにおける 10 の脆弱性に対する GUARDIAX の防御性能は以下のとおりであった。

表 5-1 OWASP Top 10 に対する GUARDIAX の防御性能

OWASP Top10	対応	備考
1. インジェクション	◎	
2. 認証の不備	◎	
3. 機密データの露出	◎	
4. XML 外部実態参照	◎	
5. アクセス制御の不備	◎	
6. 不適切なセキュリティ設定	○	Web サーバー側の設定によって制御すべき点もあり、WAF 単体で防御できないものもある。最適な設定の検証方法としては、ホスト型診断（内部診断、認証スキャンと呼称するベンダーも）によって不適切なセキュリティ設定を検出し、その結果を Web サーバー側で対処するか、WAF で対処するかを検討する手法がある。
7. クロスサイト・スクリプティング	◎	
8. 安全でないデシリアライゼーション	◎	
9. 既知の脆弱性を持つコンポーネントの使用	○	Web セキュリティのレイヤーでは Web アプリケーションの作り方によって内部コンポーネントは（結果的に）隠されていることもあり、Web サーバーを構成する各コンポーネントに

OWASP Top10	対応	備考
		既知脆弱性が存在するかは検出・制御できない可能性がある。各コンポーネントの既知脆弱性の検出と対応にはネットワーク（プラットフォーム）診断やホスト型診断を併用し、その結果から Web サーバー側で対処するか、WAF で対処するかを検討する手法がある。
10. 不十分なロギングとモニタリング	○	WAF に必要十分なログ出力機能を実装することと併せて、それを解析・モニタリングするログ分析基盤の利用が必要である。

（凡例）◎：GUARDIAX 単体で対応可能、○：GUARDIAX＋別機能で対応可能

また、OWASP Top 10 で示された以外の脆弱性に対する GUARDIAX の防御性能を表 5-2 に示す。

表 5-2　OWASP Top 10 以外の脆弱性に対する GUARDIAX の防御性能

OWASP Top 10 以外の脆弱性	対応	備考
リソースの位置を推測	◎	
HTTP リクエストスマグリング	◎	
プラットフォームの脆弱性をついた DoS 攻撃	○	攻撃手法によっては WAF が一部検知することもあるが、一般的にはプラットフォーム（ネットワーク層）における攻撃検知には IDS/IPS 機能を併用する必要がある。また、大量トラフィックによる攻撃は防御システム単体では対応不可であり、DDoS 対策オプション機能を利用することで対応。
少数 IP アドレスからの DoS 攻撃	○	大量トラフィックによる攻撃は WAF 防御単体では対応不可。DDoS 対策オプション機能を利用することで対応。
多数 IP アドレスからの DDoS 攻撃	○	大量トラフィックによる攻撃は WAF 防御単体では対応不可。DDoS 対策オプション機能を利用することで対応。
スキャニング検出	◎	
PHP インジェクション	◎	
ローカルファイルインクルード	◎	
Java 攻撃防御	◎	
EC-CUBE 防御	◎	GUARDIAX による独自対応。EC-CUBE 社とも連携が図られている。

（凡例）◎：GUARDIAX 単体で対応可能、○：GUARDIAX＋別機能で対応可能

これらの結果に基づいて、実検証を行うことで検証項目の確認を行った。本文書では、一部の攻撃に対する検証結果のみ示す。表 5-3 では OWASP Top 10 の「1. インジェクション」に対する防御性能として、SQL インジェクション及び OS コマンド・インジェクションに対する防御性能を確認した結果（抜粋版[7]）を示す。今回の実検証にて攻撃を試行したインジェクションに関する攻撃文字列に対して、GUARDIAX は「BLOCK」、すなわち攻撃を防御していることが確認できた。

表 5-3　インジェクションに対する防御性能確認結果（抜粋）

攻撃種別	攻撃文字列	攻撃文字列の説明	結果
SQL インジェクション	'OR'A'='A	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列 例）"SELECT * FROM hoge WHERE id='". $id. "';" ※ $id は文字列を想定	BLOCK
	'OR 1=1	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列	BLOCK
	'OR 1=1--	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列	BLOCK
	';update pet set kind='AAAA' where id=1001	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列	BLOCK
	'; update pet set kind=CAST(0x48494a AS VARCHAR(2000)) where id=1001--	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列（シングルクオートを使わず文字列指定を行うパターン）	BLOCK
	'u%pdate+pet+se%t+kind=CAS%T(0x414243+A%S+VARCHA%R(2000))+w%here+id%3D1001--	シングルクオートに続く SQL クエリの挿入を試みる攻撃文字列（WAF のバイパスを試みるために空白代わりの+と、無効な%を使用しているパターン）	BLOCK
	1OR 1=1	SQL クエリの挿入を試みる攻撃文字列 例）"SELECT * FROM hoge WHERE id=". $id. ";"	BLOCK

[7] 今回の有効性検証では約 600 件の攻撃文字列を生成し、防御性能を確認したところ、すべての攻撃文字列を検出したことを確認した。

攻撃種別	攻撃文字列	攻撃文字列の説明	結果
		※$id は数値を想定	
	1 update pet set kind='AAAA' where id=1001	SQL クエリの挿入を試みる攻撃文字列	BLOCK
	1 update pet set kind=123 where id=1001	SQL クエリの挿入を試みる攻撃文字列	BLOCK
	1 update pet set kind=CAST(0x48494a AS VARCHAR(2000)) where id=1001	SQL クエリの挿入を試みる攻撃文字列（シングルクオートを使わず文字列指定を行うパターン）	BLOCK
OS コマンド・インジェクション	;rm -r /	セミコロンに続くルートディレクトリ削除コマンドの挿入を試みる攻撃文字列	BLOCK
	;/sbin/sendmail test@example.jp	セミコロンに続く sendmail の実行を試みる攻撃文字列	BLOCK
	;/bin/rm -r /	セミコロンに続くルートディレクトリ削除コマンドの挿入を試みる攻撃文字列	BLOCK

（「BLOCK」とは、当該リクエストを遮断（防御）したことを示す。）

また、表 5-4 に OWASP Top 10 の「5. アクセス制御の不備」に対する防御性能として、パストラバーサルに対する防御性能を確認した結果（抜粋版）を示す。今回の実検証にて攻撃を試行したパストラバーサルに関する攻撃文字列に対して、GUARDIAX は「BLOCK」、すなわち攻撃を防御していることが確認できた。

表 5-4　アクセス制御の不備に対する防御性能確認結果（抜粋）

攻撃種別	攻撃文字列	攻撃文字列の説明	結果
パストラバーサル	../../../../../etc/passwd	/etc/passwd の本文取得を試みる攻撃文字列	BLOCK
	../../../../../abc	ファイル abc（パス不明）の本文取得を試みる攻撃文字列	BLOCK
	../../../../../aa	ファイル aa（パス不明）の本文取得を試みる攻撃文字列	BLOCK

攻撃種別	攻撃文字列	攻撃文字列の説明	結果
	../../../../../a	ファイル a（パス不明）の本文取得を試みる攻撃文字列	BLOCK
	../../../../../etc/passwd	/etc/passwd の本文取得を試みる攻撃文字列	BLOCK

（「BLOCK」とは、当該リクエストを遮断（防御）したことを示す。）

また、表 5-5 に OWASP Top 10 の「7. クロスサイト・スクリプティング」に対する防御性能として、クロスサイト・スクリプティングに対する防御性能を確認した結果（抜粋版）を示す。今回の実検証にて攻撃を試行したクロスサイト・スクリプティングに関する攻撃文字列に対して、GUARDIAX は「BLOCK」、すなわち攻撃を防御していることが確認できた。

表 5-5　クロスサイト・スクリプティングの不備に対する防御性能確認結果（抜粋）

攻撃種別	攻撃文字列	攻撃文字列の説明	結果
クロスサイト・スクリプティング	<script>alert(1)</script>	javascript コード alert(1) の挿入を試みる攻撃文字列	BLOCK
	javascript:alert(1)	javascript コード alert(1) の挿入を試みる攻撃文字列	BLOCK
	"onmouseover=alert(1)//	ダブルクオートに続く onmouseover イベントとして javascript コード alert(1) の挿入を試みる攻撃文字列	BLOCK
	alert(document.cookie)	cookie 情報を表示する javascript コードの挿入を試みる攻撃文字列	BLOCK
	<iframe src=www.yahoo.co.jp></iframe>	iframe で外部サイト(ここでは www.yahoo.co.jp)を表示するよう試みる攻撃文字列	BLOCK

（「BLOCK」とは、当該リクエストを遮断（防御）したことを示す。）

（付記）なお、表 5-3 から表 5-5 に示した攻撃文字列に対する GUARDIAX の防御性能について、複数の他社製 WAF との比較を行ったとする製品ベンダー提供のデータは、比較対象の他社製 WAF は上記の攻撃文字列に対して防御できなかった、としている。

また、クレジットカード情報データについては、通常イベント詳細画面で確認できるレスポンスデータ欄が空欄になっていることを確認した。これは、その番号を WAF の管理者やユーザーが閲覧できないように配慮したためと考えられる。

5.1.2　検証項目 1-2 の検証結果

(1) 検証項目の内容

偽陽性が少ないか

(2) 検証結果

製品ベンダーから提供されたデータに基づいて、偽陽性が少ないことを確認した。

(3) 検証内容の詳細

製品ベンダーによるデータや記録に基づき評価を行った。OWASP Top 10 への防御性能をベースに、攻撃文字列に似せた文字列(正常なリクエスト)に基づいてアクセスすることで、それを誤って防御することが無いかの確認を行った。表 5-6 では OWASP Top 10 の「1. インジェクション」に関する偽陽性の少なさの確認結果を示している。今回評価を行った範囲では、SQL インジェクションに似せた文字列（攻撃文字列ではない）をリクエストしても、そのリクエストを誤って遮断することが無いことを確認した。

表 5-6　SQL インジェクションに関連する偽陽性の少なさの確認結果

関連する攻撃種別	文字列	文字列の説明	結果
SQL インジェクション	`or 1`	攻撃文字列ではない。攻撃コードの断片とも読めるが、実行はできない。	THRU
	`union select`	攻撃文字列ではない。攻撃コードの断片とも読めるが、実行はできない。	THRU
	`union 1 select`	攻撃文字列ではない。攻撃コードの断片とも読めるが、実行はできない。	THRU
	`union`	攻撃文字列ではない。攻撃コードの断片とも読めるが、実行はできない。	THRU
	`select`	攻撃文字列ではない。攻撃コードの断片とも読めるが、実行はできない。	THRU
	`M'cintosh and Johnson`	攻撃文字列ではない。シングルクオートと and があるが単なる文字列である。	THRU

関連する攻撃種別	文字列	文字列の説明	結果
	select uion	攻撃文字列ではない。攻撃コードの断片（uion）とも読めるが、実行はできない。	THRU
	G.M. union select the option	攻撃文字列ではない。攻撃コードの断片（union select）とも読めるが、実行はできない。	THRU

（「THRU」とは、当該リクエストを遮断せず通過させたことを示す。）

表 5-7 では OWASP Top 10 の「5. アクセス制御の不備」の脆弱性のうちパストラバーサルに関する偽陽性の少なさの確認結果を示している。今回評価を行った範囲では、パストラバーサルに似せた文字列（攻撃文字列ではない）をリクエストしても、そのリクエストを誤って遮断することが無いことを確認した。

表 5-7　パストラバーサルに関連する偽陽性の少なさの確認結果

関連する攻撃種別	文字列	文字列の説明	結果
パストラバーサル	../../../../../	攻撃文字列ではない。パストラバーサル特有の文字列だが、ファイルが指定されていないため攻撃が成立しない。	THRU
	../../	攻撃文字列ではない。パストラバーサル特有の文字列だが、ファイルが指定されていないため攻撃が成立しない。	THRU
	../..	攻撃文字列ではない。パストラバーサル特有の文字列だが、ファイルが指定されていないため攻撃が成立しない。	THRU
	../	攻撃文字列ではない。パストラバーサル特有の文字列だが、ファイルが指定されていないため攻撃が成立しない。	THRU

（「THRU」とは、当該リクエストを遮断せず通過させたことを示す。）

表 5-8 では OWASP Top 10 の「7. クロスサイト・スクリプティング」に関する偽陽性の少なさの確認結果を示している。今回評価を行った範囲では、クロスサイト・スクリプティングに似せた文字列（攻撃文字列ではない）をリクエストしても、そのリクエストを誤って

遮断することが無いことを確認した。

表 5-8　クロスサイト・スクリプティングに関連する偽陽性の少なさの確認結果

関連する攻撃種別	文字列	文字列の説明	結果
クロスサイト・スクリプティング	alert(1)	攻撃文字列ではない。javascript コードと読めなくもないが、単なる文字列である。	THRU
	script alert(1) script	攻撃文字列ではない。HTML タグ<>が除去された javascript コードと読めなくもないが、単なる文字列である。	THRU
	script alert(1)	攻撃文字列ではない。HTML タグ<>が除去された javascript コードと読めなくもないが、単なる文字列である。	THRU
	script alert()	攻撃文字列ではない。HTML タグ<>が除去された javascript コードと読めなくもないが、単なる文字列である。	THRU
	script alert	攻撃文字列ではない。HTML タグ<>が除去されているが、それを考慮しても javascript コードとしても成立していない単なる文字列である。	THRU
	javascript:という書き方は	攻撃文字列ではない。"javascript:"の文字列だけで攻撃文字列と誤認していないか？	THRU
	/echo.asp?a=%2bADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAxACkAPAAvAHMAYwByAGkAcAB0AD4ADQAK-	攻撃文字列ではない。/echo.asp に渡されているパラメータ a をデコードすると、"<script>alert(1)</script>"（先頭のスペース以外の文字は NULL を含む 2 バイト文字）となるが、これを攻撃文字列とするかは WAF 側ではなく Web アプリケーション側の問題と考えられる。	THRU

関連する攻撃種別	文字列	文字列の説明	結果
	aaa	攻撃文字列ではない。HTML タグを含む文字列だが、javascript タグの挿入ではない。	THRU

（「THRU」とは、当該リクエストを遮断せず通過させたことを示す。）

（付記）なお、表 5-6 から表 5-8 に示した攻撃文字列に似せた文字列に対する GUARDIAX の対応結果（偽陽性の少なさ）について、複数の他社製 WAF との比較を行ったとする製品ベンダー提供のデータは、通常攻撃が行われる箇所と同一箇所に対して攻撃文字列に似せた文字列をリクエストした際、比較対象の他社製 WAF は上記文字列を誤って攻撃文字列として検知・防御してしまった、としている。

5.1.3 検証項目 1-3 の検証結果

(1) 検証項目の内容

SaaS 版とコンテナ版に性能の差異は存在しないか

(2) 検証結果

SaaS 版とコンテナ版に性能の差異は存在しないことを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングの結果、コンテナ版と SaaS 版は同じエンジンや管理画面にて実装しているため、防御性能やダッシュボードに差分はないとの回答を得た。

5.1.4 検証項目 1-4 の検証結果

(1) 検証項目の内容

ダッシュボードにおいて攻撃の有無を確認できるか

(2) 検証結果

ダッシュボードにおいて攻撃の有無を確認できた。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。攻撃試行を行った後のダッシュボードの画面を図 5-1 及び図 5-2 に示す。ダッシュボードの Top 画面において、検知した攻撃件数と脅威度の割合、タイムライン、攻撃元国別 Top5、攻撃元 IP アドレスの Top5、攻撃元マップを視

覚的に確認できた。

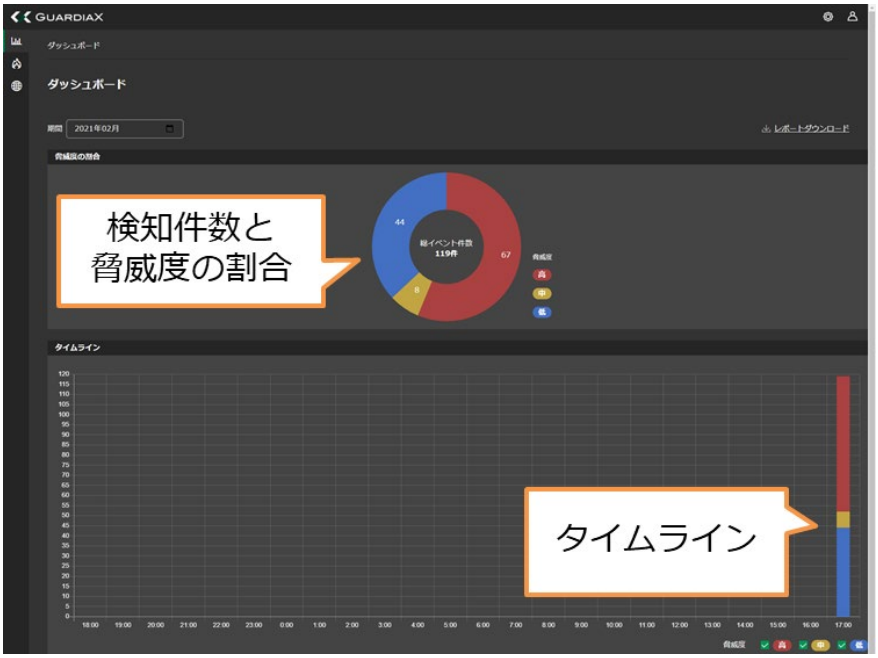


図 5-1　ダッシュボードにおける攻撃検知件数・タイムラインの表示

図 5-2　ダッシュボードにおける攻撃元国・IP アドレス、攻撃元マップの表示

検知した攻撃の一覧については、図 5-3 に示すとおりダッシュボードの「イベント」から確認できた。一覧では、タイムスタンプ（攻撃を検知した日時)、脅威度、攻撃元 IP、攻撃先ホスト、パス、攻撃種類、WAF が実行したアクション（検知のみ／通信のブロック）を確認することができる。図 5-3 上部にあるとおり、期間、脅威度、攻撃元 IP 等による絞り込みも可能であった。また、検知した攻撃一覧は CSV で出力することが可能であった。

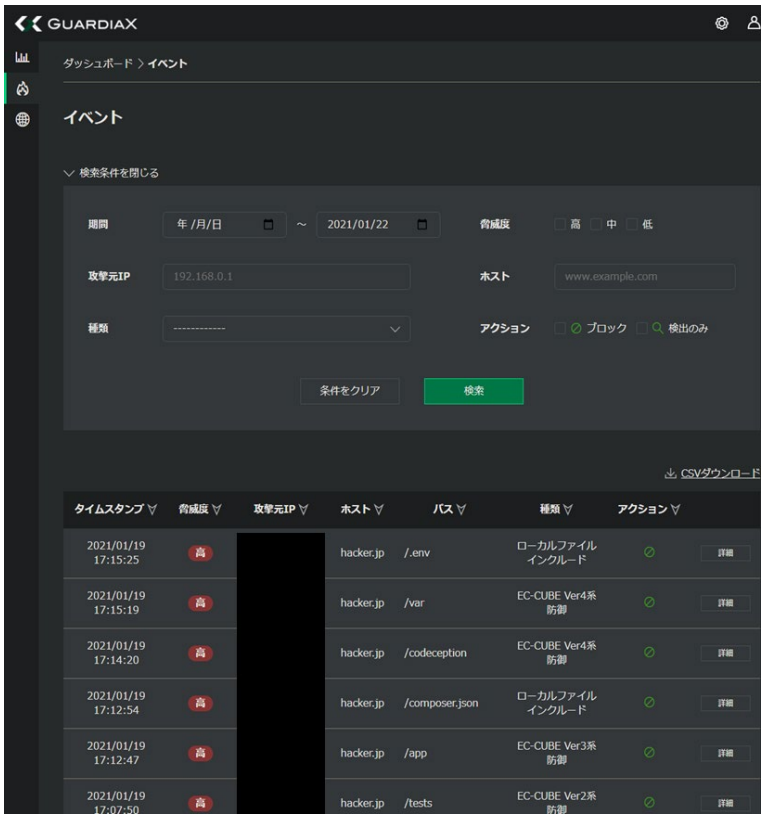


図 5-3　検知した攻撃一覧の表示

5.1.5　検証項目 1-5 の検証結果

(1) 検証項目の内容

ダッシュボードにおいて検知した攻撃の詳細を確認できるか

(2) 検証結果

ダッシュボードにおいて検知した攻撃の詳細を確認できた。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。図 5-3 で示されるイベント一覧から、あるイベントを選択した画面を図 5-4 に示す。この画面では、クロスサイト・スクリプティングを検知した際のイベント詳細を示している。この図から明らかなように、攻撃を検出した時間、脅威度、攻撃元国名、攻撃元 IP、攻撃元ホスト、攻撃のコード（パス）、攻撃の種類、WAF が行ったアクション（検知のみ／通信のブロック）、WAF が攻撃と判断したコード（検知コード）を確認することができた。また、図 5-5 に示すとおり、それぞれのイベントにおけるリクエスト（攻撃元から送信された通信データ）とレスポンス（Web サイトが返信した通信データ）も確認することができた。

図 5-4　検知した攻撃に関する表示（クロスサイト・スクリプティングの場合）

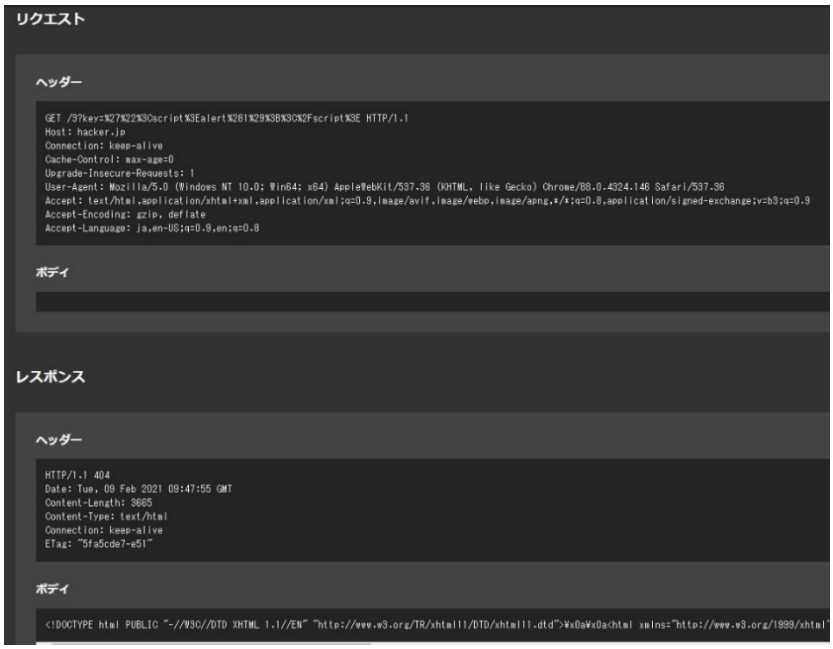


図 5-5　検知した攻撃のリクエスト・レスポンスの表示
（クロスサイト・スクリプティングの場合）

クレジットカード情報データのレスポンスに関する GUARDIAX の検出結果を図 5-6 に示す。レスポンスに対するイベントについても、攻撃を検出した時間、脅威度、攻撃元国名、攻撃元 IP、攻撃元ホスト、攻撃のコード（パス）、攻撃の種類、WAF が行ったアクション（検知のみ／通信のブロック）、WAF が攻撃と判断したコード（検知コード）を確認することができた。また、図 5-7 に示すとおり、それぞれのイベントにおけるリクエスト（攻撃元から送信された通信データ）とレスポンス（Web サイトが返信した通信データ）も確認することができた。この図から明らかなように、機密情報保護のため、クレジットカード情報はダッシュボードからは確認できない形式となっていた。

図 5-6　検知した攻撃に関する表示（クレジットカード情報データのレスポンスの場合）

図 5-7　検知した攻撃のリクエスト・レスポンスの表示
（クレジットカード情報データのレスポンスの場合）

5.1.6　検証項目 1-6 の検証結果

(1) 検証項目の内容

ダッシュボードにおいて検知した攻撃のレベル分けができるか

(2) 検証結果

検知した攻撃の脅威レベルは 3 段階でレベル分けがされていた。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。前述のとおり、検出した攻撃イベントのそれぞれに対して脅威度が設定された。脅威度は高・中・低の 3 段階で分類され、今回の検証より、以下のような分類が存在すると想定された。

- 脅威度 低：スキャニング検出
- 脅威度 中：クレジットカード情報を除くレスポンスでの検知（SQL エラー、Java 情報、PHP 情報、IIS 情報、ディレクトリ情報、CGI 情報）
- 脅威度 高：その他の攻撃種別、及びクレジットカード情報データのレスポンス

5.1.7 検証項目 1-7 の検証結果

(1) 検証項目の内容

ダッシュボードにおいて Web サイトの脆弱性を指摘するか

(2) 検証結果

情報漏えいに関する Web サイトの脆弱性を指摘できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。GUARDIAX では Web サイトから送信される HTTP レスポンスに特定の機密情報（クレジットカード番号等）が含まれていた場合に、それを検知する機能があった。そのため、攻撃者に有用な詳細な SQL エラー情報を表示してしまう等、情報漏えいに関する Web サイトの脆弱性を指摘すると考えられる。ただし、脆弱性診断ツールのように多数の脆弱性を発見することを目的としたものではなく、WAF から Web サイトへ疑似攻撃を行い脆弱性の有無を調査するものではないことに留意が必要である。

5.2 運用性に関する検証結果

5.2.1 検証項目 2-1 の検証結果

(1) 検証項目の内容

防御ルールの設定変更の反映のタイミングを設定できるか

(2) 検証結果

基本的に設定変更はリアルタイムで反映されることを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングの結果、ユーザーが防御ルールを変更した場合に、基本的にリアルタイムで変更されるが、回線状況や設定作業の処理負荷によっては、反映までに数分掛かることがあるとの回答を得た。

5.2.2 検証項目 2-2 の検証結果

(1) 検証項目の内容

攻撃情報は分かり易いか

(2) 検証結果

ダッシュボードにおいて有用な攻撃情報を把握できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。ダッシュボード上でイベントの脅威度の割合、タイムラインを確認できるため、攻撃の大まかな概要と、攻撃を受けている時刻の傾向、集中度等を視覚的に把握できることを確認した。また、国別、IP 別の攻撃元ランキングから、特定の国や IP からのアクセスを制限する際に役立つ情報を得ることができた。

5.2.3 検証項目 2-3 の検証結果

(1) 検証項目の内容

ログ分析は分かり易いか

(2) 検証結果

ダッシュボードにおいて有用なログ分析情報を把握できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。イベント詳細画面において、HTTP リクエスト及びレスポンスのヘッダー・ボディを確認できるため、検知された通信の具体的な内容が確認できた。一部のイベントについては、イベント詳細画面の検知コード欄にシグニチャがマッチしたと思われる文字列など、より詳細な情報を確認することができるため、万が一誤検知が発生したと思われる場合にも有用な情報を得ることができると考えられる。

5.2.4 検証項目 2-4 の検証結果

(1) 検証項目の内容

防御ルールの更新連絡は存在するか

(2) 検証結果

検知項目の増減がある場合に更新連絡があることを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングにより、検知項目の増減がある場合はユーザーにアナウンスがあり、検知項目内の詳細変更についてはアナウンスされないことを確認した。

5.2.5 検証項目 2-5 の検証結果

(1) 検証項目の内容

障害時の復旧対応が準備されているか

(2) 検証結果

障害時の復旧対応が準備されていることを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングにより、冗長構成となっており、復旧対応を準備することで常時稼働しているとの回答を得た。

5.2.6 検証項目 2-6 の検証結果

(1) 検証項目の内容

当該製品の活用方法を容易に習得できるか

(2) 検証結果

当該製品の活用方法を容易に習得できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。直感的な UI のダッシュボードが実装されているほか、別途マニュアルも用意されているため、活用方法の習得は容易であった。

5.2.7 検証項目 2-7 の検証結果

(1) 検証項目の内容

今後の事業方針・目標は明確か

(2) 検証結果

グループ企業内のシナジーを活かした事業方針が存在することを確認した。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングによって、グループ企業内のシナジーを活かし、より安定的かつ先進的なサービスを目指しているとの回答を得た。

5.2.8 検証項目 2-8 の検証結果

(1) 検証項目の内容

製品機能・性能の向上に向けた拡張性、他製品との連携の予定はあるか

(2) 検証結果

外部の統合ログ分析機器との連携やコミュニケーションツールとの連携を予定しているとのことであった。

(3) 検証内容の詳細

本検証項目は製品ベンダーに対するヒアリングによって確認した。ヒアリングによって、外部の統合ログ分析機器と GUARDIAX の検知ログの連携機能を実装する予定との回答を得た。また、今後コミュニケーションツールへの連携も予定しているとのことであった。

5.3 導入容易性に関する検証結果

5.3.1 検証項目 3-1 の検証結果

(1) 検証項目の内容

導入する Web サイトやサーバーに制約条件はあるか

(2) 検証結果

本検証の範囲では、導入する Web サイトやサーバーにおける条件は確認できなかった。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。本検証の範囲では制約となる条件は確認できなかった。一般的な Web サイトやサーバーであれば制約は受けないと想定される。

5.3.2　検証項目 3-2 の検証結果

(1) 検証項目の内容

導入に至るまでの手続きは簡単か

(2) 検証結果

導入に至るまでの手続きは簡単であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。アカウント発行後、利用開始までの手続きは利用者側操作のみで可能であった。また、利用開始の手続き自体も比較的簡潔であるため、手続きは簡単であった。

5.3.3　検証項目 3-3 の検証結果

(1) 検証項目の内容

導入時の設定は簡単か

(2) 検証結果

初期設定は Web GUI 上で簡単に設定可能であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。対象の Web サイト（ドメイン）を追加する際、図 5-8 に示すように 1 画面の設定で多くの初期設定が完了した。

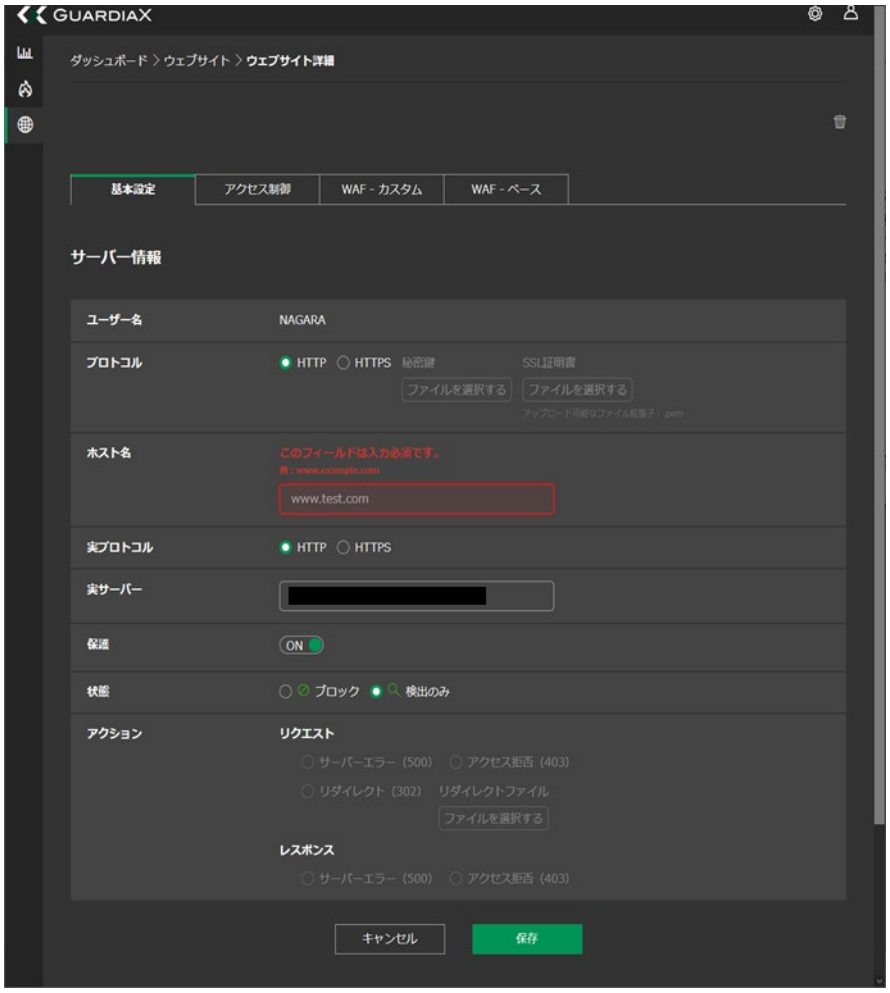


図 5-8　Web サイト設定画面

Web サイトへのトラフィックを GUARDIAX 経由に変更するために必要な DNS の変更についても、アカウント案内等に記載されていたため、設定は容易であった。また、ルール追加等のカスタマイズについて、ダッシュボード上で各 Web サイト（ドメイン）別の設定が可能であった。

Web サイト毎にページが用意されており、「基本設定」、「アクセス制限」、「WAF-カスタム」、「WAF-ベース」の 4 つの設定メニューが存在した。「基本設定」は図 5-8 で示す画面である。アクセス制限（フィルタリングルール追加）の設定画面を図 5-9 に示す。この設定画面では、各ドメイン及びサイト内の詳細なフィルタリングルールを作成できた。

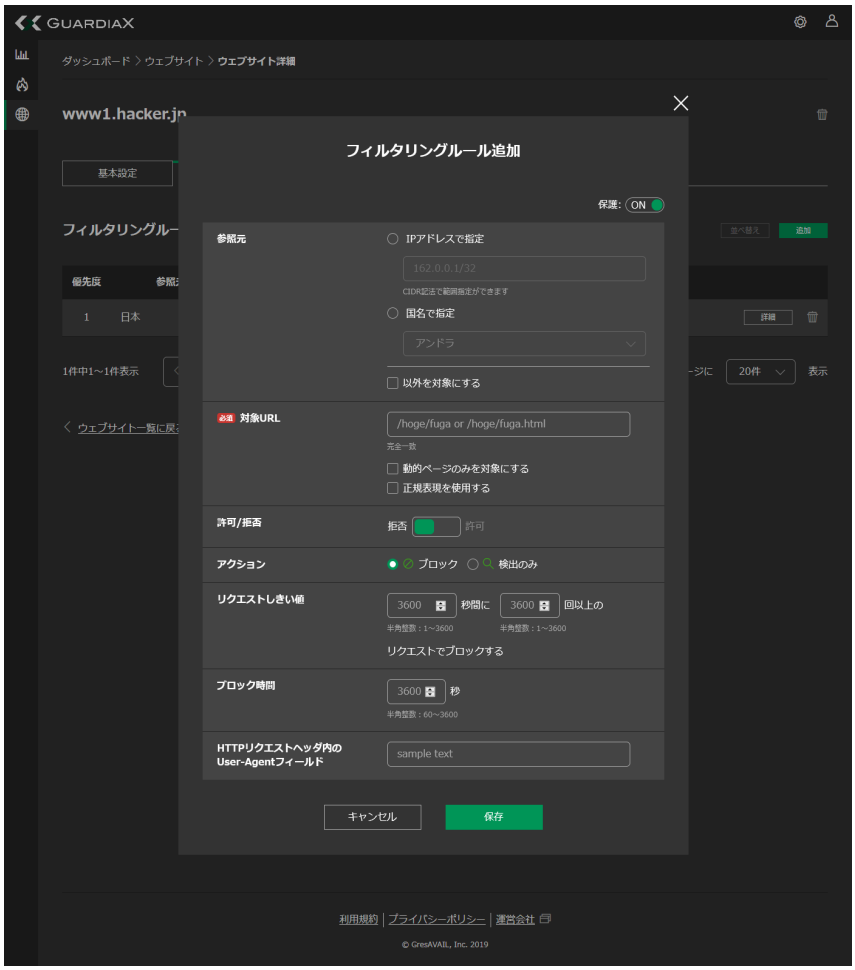


図 5-9　フィルタリングルール追加の設定画面

WAF-カスタムの設定画面を図 5-10 に示す。この設定画面では、組込みのシグネチャに加え、GUARDIAX で検出・ブロックを行う指標となるカスタムシグネチャを追加できた。

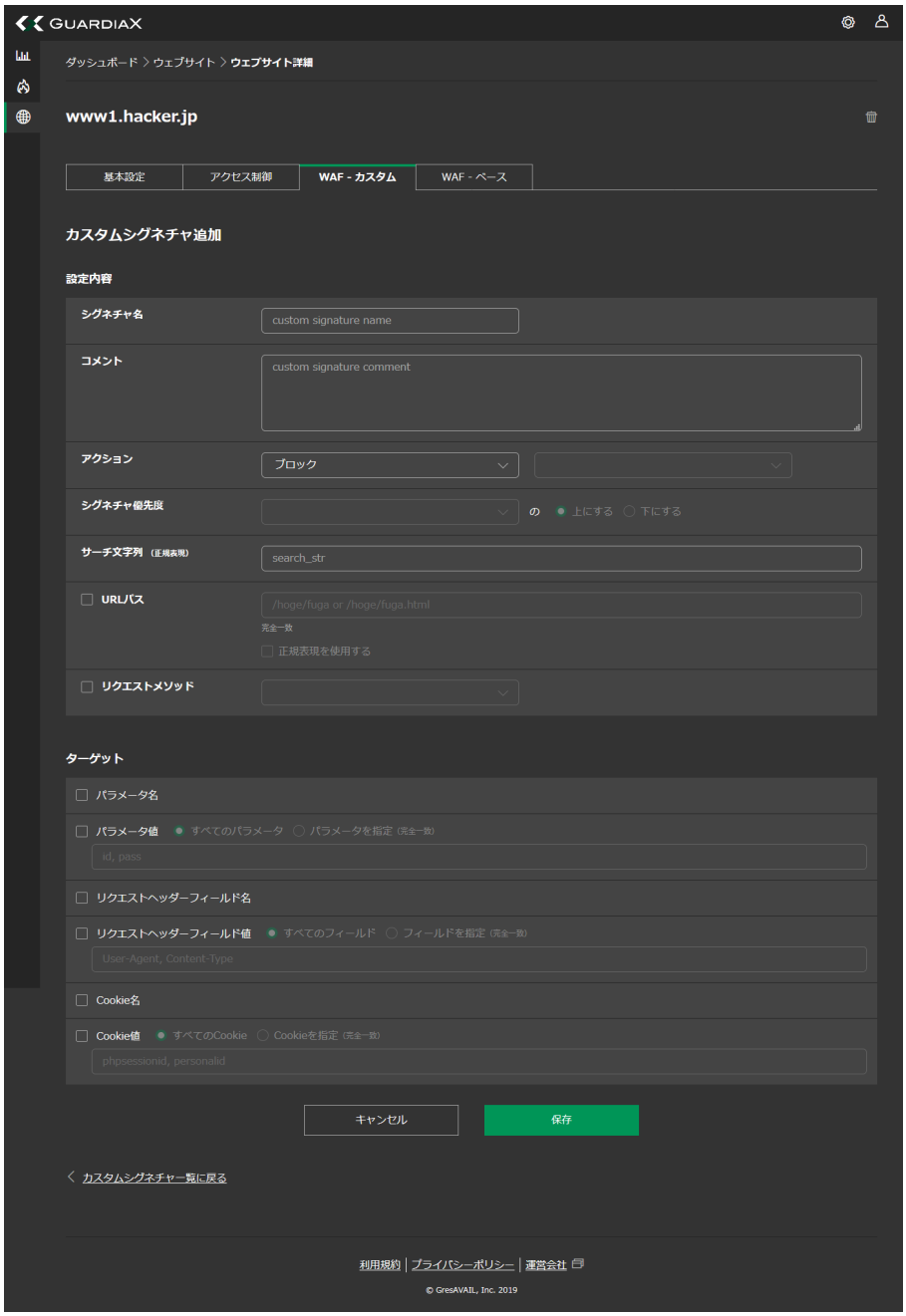


図 5-10　カスタムシグネチャ追加設定画面

WAF-ベースの設定画面を図 5-11 に示す。この設定画面では、GUARDIAX にあらかじめ組込まれたシグネチャを検知・ブロックに利用するか否かの設定を、Web サイト毎にチェックボックス方式で設定できた。ベースシグネチャは、リクエスト防御、レスポンス保護、CMS 脆弱性の分類で複数の項目が設定されていた。リクエスト防御の分類では、Web アプリケーションの脆弱性を狙った基本的な攻撃の防御を設定することができた。レスポンス保護では、クレジットカード情報データ等の情報に関するレスポンス有無を設定することができた。CMS 脆弱性では、ショッピングサイトに広く利用されている CMS である EC-CUBE に特化した防御設定が可能であった。

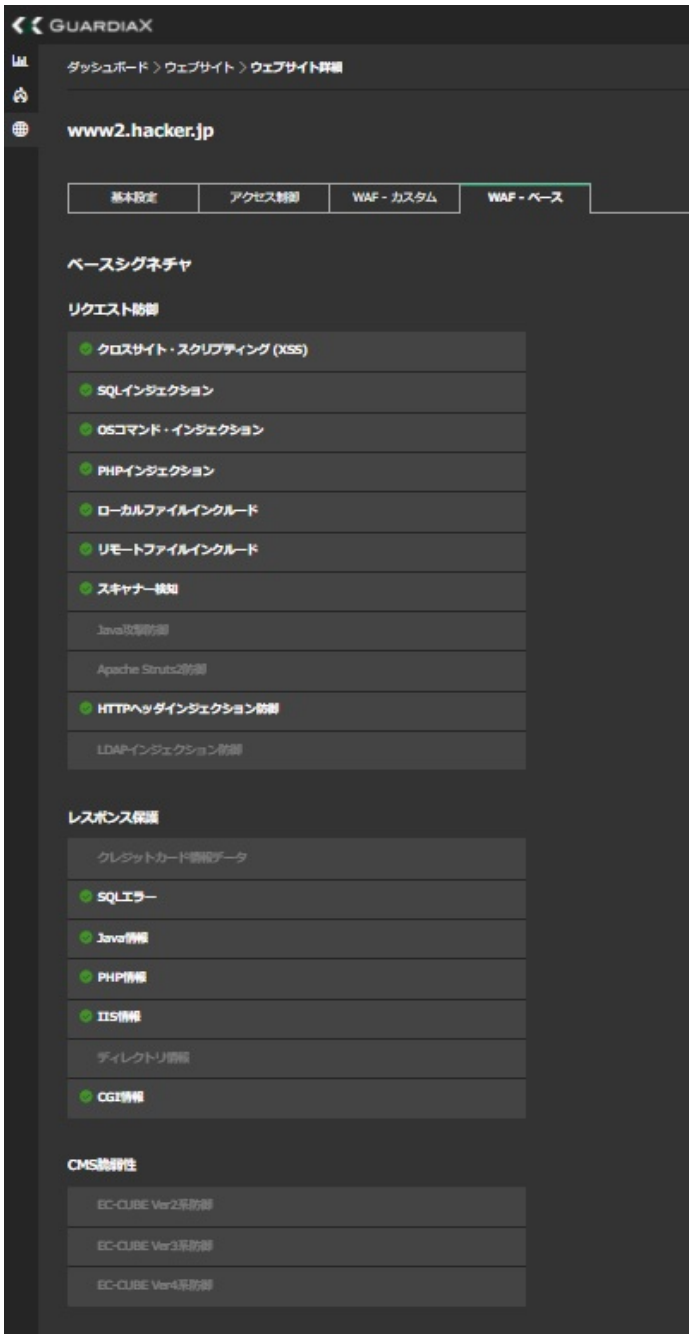


図 5-11　ベースシグネチャの設定画面

5.3.4　検証項目 3-4 の検証結果

(1) 検証項目の内容

導入に当たってサービスの停止が必要か

(2) 検証結果

導入に当たって大規模なサービス停止は不要と考えられる。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。実検証の範囲では大規模なサービス停止は不要と考えられるが、DNS 設定などの Web アプリケーション構成に依存する面が大きいことに留意が必要である。

5.3.5 検証項目 3-5 の検証結果

(1) 検証項目の内容

Web アプリケーションに対する変更が必要か

(2) 検証結果

Web アプリケーションに対する変更が不要であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証によって確認した。検証により、Web アプリケーション自体の変更は不要であることを確認した。ただし、ロードバランサーを設置している、独自にファイアウォールを設定している等の状況では、GUARDIAX からの通信を許可する、発信元 IP を正しく表示するための設定を追加[8]する等、細かな設定が必要となることに留意が必要である。

5.3.6 検証項目 3-6 の検証結果

(1) 検証項目の内容

導入までの必要期間は短期間か

(2) 検証結果

短期間で導入できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び製品ベンダーに対するヒアリングによって確認した。前述のとおり、GUARDIAX の設定は容易であり、Web アプリケーション側の設定変更を必要としないため、アカウント設定後[9]に短期間で導入可能であることを確認した。

---

[8] Web アプリケーション側のアクセスログには WAF をプロキシとして経由した通信として、発信元が同じ IP アドレスであるように記録されるケースがあるため。

[9] アカウント発行までの期間は最短 1 日、長い場合でも数営業日単位とされている。

5.3.7　検証項目 3-7 の検証結果

(1) 検証項目の内容

安全性や機密性に問題はないか

(2) 検証結果

安全性や機密性に特段の問題がないと考えられることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及び製品ベンダーに対するヒアリングによって確認した。ダッシュボードのログイン仕様について、所定の ID とパスワードを入力後、すぐにログインとはならず、登録されているメールアドレス対してログイン確認のメールが届く。メール本文に記載されているリンクをクリックすることでログインが完了する二段階認証の仕様になっていることを確認した。また、ヒアリングにより、データが GUARDIAX を通過する際に、クレジットカード番号や機密情報は GUARDIAX に保管されることは無いとの回答を得た。

6. まとめ

GUARDIAX は、Web アプリケーションの脆弱性を悪用するサイバー攻撃から Web サイトを保護する WAF 製品である。ベンダーは、WAF の防御範囲である不正ログイン試行、Web アプリケーションの脆弱性への攻撃などをブロックするだけでなく、これまでの WAF の課題であった過検知や誤検知を減少させていることが特徴であるとしている。WAF のダッシュボードでは、攻撃状況やログ、統計などを可視化しているほか、一つ一つの Web サイトにきめ細かく設定することができるため、迅速かつ適切なセルフ管理が可能である。加えて、GUARDIAX SaaS 版では、DNS 設定の切り替えだけで WAF を導入することができることも特徴として挙げられる。

今回の検証は、前述の検証環境、検証条件、方法の範囲で、GUARDIAX の 4 つの差別化ポイントとされている事項に対して、「製品機能・性能」、「運用性」、「導入容易性」の観点から検証を実施し確認した。